NAIST-IS-DD0261201

博士論文

インターネットにおける
ライフライン通信の実現に関する研究

菊地 高広

2005年2月3日

奈良先端科学技術大学院大学
情報科学研究科 情報システム学専攻

本論文は奈良先端科学技術大学院大学情報科学研究科に
博士 (工学) 授与の要件として提出した博士論文である。

菊地 高広

審査委員：　砂原 秀樹 教授
山口 英 教授
藤川 和利 助教授

インターネットにおける
ライフライン通信の実現に関する研究*

菊地 高広

内容梗概

インターネットが普及するとともに、様々な通信サービスのインフラとしての重要性が増しつつある。そうした中、緊急通報や安否情報や災害情報のやりとりなどを行なうライフライン通信についても、インターネット接続環境さえあれば利用可能であることが求められている。また、インターネット上では高度なマルチメディア環境のサポートなどによって、多くの人に利便性の高いライフライン通信サービスの提供が可能となる。

しかし、電話などの既存のメディアで行われてきたライフライン通信の機能を、インターネット上で実現するには様々な課題がある。一つ目は、適切な通信相手と通信するための接続先解決の取り扱いである。緊急通報はその場所を管轄する最寄り機関へ接続される必要があり、電話においては 110 番や 119 番のように簡易なアクセス手段で意識することなく適切な接続がなされる。また、自分が現在いる地域の災害情報を得たい場合にも、同様に適切な接続先解決が必要となる。二つ目は、発信者の識別情報の取り扱いである。緊急通報や安否情報の通知と登録では、いたずらやなりすまし防止、ならびに、呼び返しの実現が求められる。三つ目は、発信者の居場所である地理的位置情報の取り扱いである。緊急通報ではその対処や現場への駆け付けのため、発信者の居場所を把握する必要があり、安否情報においても居場所が正確に登録される必要がある。

*奈良先端科学技術大学院大学 情報科学研究科 情報システム学専攻 博士論文, NAIST-IS-DD0261201, 2005 年 2 月 3 日.

そこで、本論文では、これらの課題について、ライフライン通信をインターネットにおいて実現するための議論を行ない、それをもとにインターネットにおけるライフライン通信で用いられる共通の基盤技術の確立を目指す。そして、その基盤技術として、通信接続先解決のための地理的位置情報ベースの ENUM 方式、発信者の地理的位置情報証明書方式、および、ユーザ情報証明書方式という、各課題を解決する三つのモデルを提案する。

これらの三つの提案モデルに基づき設計したライフライン通信システムの実装構築を行ない、実証実験ならびに性能評価を行なった。その結果、このシステムは他に考えられる方式と比較してスケーラビリティやセキュリティとプライバシーの点で好ましいだけでなく、十分実用的であることを確認した。

キーワード

ライフライン通信, 緊急通報, 地理的位置, GPS, ENUM, SIP, PKI

Lifeline Communication System in the Internet*

Takahiro Kikuchi

Abstract

As the Internet spreads, it is increasing in importance as the infrastructure for various communication services. Lifeline communications such as emergency calls, registring safety information, or getting disaster information, should be available if there is the Internet connectivity. Lifeline communications over the Internet offer highly convenient services for various people with advanced multimedia support.

However, there are various problems in the realization on the Internet of the function of lifeline communications performed on traditional media such as the telephone. The first problem is the routing for lifeline communications. In an emergency call, it is necessary to connect to the nearest lifeline service agency. For example, a telephone user can start an emergency call with a simple access means such as 110 or 119. Moreover, a user needs to know the correct Internet address to connect when he wants to get any disaster information about his current location. The second problem is the handling of the identity information of the caller. In an emergency call or a registration of safety information, the caller needs to be identified in order to prevent fake calls or nuisance calls and to make a callback possible. The third problem is the handling of the geographical location information where the caller is actually located. The geographical location information of the caller is necessary when going to help in the case of an emergency call or when registering safety information.

*Doctoral Dissertation, Department of Information Systems, Graduate School of Information Science, Nara Institute of Science and Technology, NAIST-IS-DD0261201, February 3, 2005.

In this paper, I discuss these problems and aim at the establishment of a common base technology for lifeline communications over the Internet. I propose three models, the ENUM based on geographical location information model, the geographical location information certificate model, and the user information certificate model.

I have implemented the lifeline communication system with a design based on these three proposal models, and performed verification experiments and performance evaluations. The results showed that this system is sufficiently practical in respect of performance, security, privacy and scalability.

Keywords:

lifeline communication, emergency call, geographical location, GPS, ENUM, SIP, PKI

目 次

第 1 章　序論 **1**

1. インターネットにおけるライフライン通信 1
   - 1.1 インターネット上での実現 1
   - 1.2 ライフライン通信の意味 1
   - 1.3 インターネット上での実現の意義 2

2. 本研究の取り組みと位置づけ 2
   - 2.1 本研究の対象 2
   - 2.2 本研究の取り組み 3
   - 2.3 本研究の位置づけ 4

3. 本論文の構成 4

第 2 章　ライフライン通信とインターネット **5**

1. ライフライン通信の種類 5
   - 1.1 緊急通報型 5
   - 1.2 安否連絡型 6
   - 1.3 安否登録・検索型 6
   - 1.4 情報取得・提供型 6

2. ライフライン通信で必要とされる機能 7
   - 2.1 緊急通報型 7
     - 2.1.1 適切な通報先への接続 7
     - 2.1.2 発信者の特定識別 7
     - 2.1.3 発信者の位置情報の通知 8
     - 2.1.4 優先取扱いによる通信品質確保 8
     - 2.1.5 対応すべき機能のまとめ 10

2.2 安否連絡型 11
2.3 安否登録・検索型 11
2.4 情報取得・提供型 12
2.4.1 適切な情報取得先への接続 12
2.4.2 発信者の位置情報の通知 14
2.5 ライフライン通信で必要とされる機能 14
3. インターネットと PSTN 16
3.1 ネットワークと端末の位置付け 16
3.2 識別子とルーティング 16
3.3 インターネットにおける識別子 17
3.4 管理把握体制の違い 18
4. 既存技術と問題点 18
4.1 ENUM による接続先解決 19
4.2 HTTP/SIP ヘッダによる位置情報通知 20
4.3 位置情報登録管理システム 20
4.4 DHCP による位置情報提供 20
4.5 DNS による位置情報登録と提供 21

第 3 章 ライフライン通信のための要求事項 23

1. ライフライン通信の接続先解決 23
1.1 特番と一般電話番号 23
1.2 インターネット上でのサービス 24
1.3 サービスによる管轄地域区分の違い 25
1.4 接続先解決における要求事項 25
2. 発信者の地理的位置情報の取扱い 26
2.1 地理的位置情報の必要性 26
2.2 地理的位置情報のプライバシー 27
2.3 GPS による地理的位置情報 27
2.4 地理的位置情報に関する要求事項 28
3. 発信者のユーザ情報の取扱い 29

3.1 ユーザ識別子の必要性 29
3.2 インターネットにおけるユーザ識別子 29
3.3 ユーザ識別子を付与する対象 30
3.4 ユーザ識別子の正当性 31
3.5 ユーザ情報に関する要求事項 32

第 4 章 提案方式 **33**
1. 地理的位置情報ベースの ENUM 33
1.1 ENUM のしくみ 33
1.2 ENUM の枠組みの応用 35
2. 地理的位置情報証明書 36
2.1 網からのおよその位置情報の提供と保証 36
2.2 地理的位置情報証明書の発行 37
2.3 地理的位置情報証明書の通知と検証 38
2.4 地理的位置情報証明書と GPS 情報 40
3. ユーザ情報証明書 41
3.1 ユーザ情報証明書の発行 41
3.2 ユーザ情報証明書の通知と検証 42

第 5 章 ライフライン通信システム **45**
1. システム構成 45
1.1 接続先情報管理サーバ 46
1.2 地理的位置情報管理サーバ 46
1.3 ユーザ情報管理サーバ 47
1.4 地理的位置情報証明書の入手 47
1.5 ユーザ情報証明書の入手 47
1.6 接続先解決と証明書通知 47
1.7 各証明書の検証 48
2. ライフライン通信の流れ 48
2.1 発信側端末の起動 48

2.1.1 IP アドレスの取得 50
2.1.2 SIP における登録 50
2.1.3 地理的位置情報の取得 50
2.2 ライフライン通信の接続先解決 51
2.2.1 ユーザからのライフライン通信呼び出し 51
2.2.2 接続先情報リストの取得 52
2.2.3 接続先情報リストからの選択 53
2.3 ライフライン通信の接続と通知 53
2.3.1 SIP によるライフライン通信リクエスト 53
2.3.2 最新情報の取得 54
2.3.3 取得した最新情報の通知 54
2.4 ライフライン通信の受信と検証 55
2.4.1 発信者情報通知の受信 55
2.4.2 地理的位置情報証明書の検証 56
2.4.3 ユーザ情報証明書の検証 58
2.5 ライフライン通信の確立 60
2.6 ライフライン通信の切断 60
3. システムの運用 60
3.1 IP アドレス空間に対するルート CA 60
3.2 ドメイン名に対するルート CA 62
3.3 階層構造にそった中間 CA の配置 63
3.4 各証明書の有効性と失効管理 64
3.4.1 地理的位置情報証明書 64
3.4.2 ユーザ情報証明書 64
3.4.3 IP アドレス空間公開鍵証明書 64
3.4.4 ドメイン名公開鍵証明書 65
3.4.5 証明書失効リストの確認 65
3.5 接続先解決機構における運用 66
3.5.1 災害時等の迂回対策 66

3.5.2 DNS 障害時への対策 67
4. システムの拡張 67
4.1 モバイル IP への対応 68
4.2 地理的位置情報証明書の拡張 68

第 6 章 システム評価 **71**
1. システム性能評価 71
1.1 証明書の鍵長に対する所要時間 71
1.2 証明書内のデータ長に対する所要時間 72
1.3 証明書の取り扱いにおけるシステム性能 73
1.4 ライフライン通信確立における所要時間分析 74
2. システムの性質評価 76
2.1 システムのスケーラビリティ 77
2.1.1 地理的位置情報管理サーバの配置 77
2.1.2 ユーザ情報管理サーバの配置 77
2.2 セキュリティとプライバシー 78
2.3 システムのリスクと頑健性 78
2.3.1 発信者側での要件 78
2.3.2 接続先側での要件 79
2.3.3 地理的位置情報管理サーバと通信できない場合 . 79
2.3.4 ユーザ情報管理サーバと通信できない場合 79
2.3.5 接続先の名前解決ができない場合 80
2.3.6 最小限構成での動作 80
2.4 本提案の証明書方式の評価 80
2.4.1 インターネット標準との親和性 80
2.4.2 証明書の検証 81
2.4.3 ユーザ端末における証明書の取り扱い 81
2.4.4 再利用の防止 81
2.4.5 通信記録としての証明書 81
2.4.6 二つの証明書の分離 82

3. 他の方式との比較評価 82
3.1 接続先解決方式における比較評価 82
3.1.1 IP ルーティング方式 83
3.1.2 DHCP サーバなどから情報提供する方法 84
3.1.3 集中受付ゲートウェイ方式 85
3.1.4 ENUM 以外の枠組み利用 85
3.1.5 プロキシサーバで接続先解決する方式 86
3.2 地理的位置情報の取扱い方式における比較評価 87
3.2.1 網側から情報提供しない方式 87
3.2.2 DNS による情報提供方式 87
3.2.3 DHCP による情報提供方式 88
3.2.4 ユーザによる情報通知方式 89
3.2.5 サーバへの問い合わせ方式 89
3.3 ユーザ情報の取扱い方式における比較評価 91
3.3.1 サーバへの問い合わせ方式 91
3.3.2 ユーザ公開鍵証明書方式 91

第 7 章 研究の総括 **93**
1. 本研究によって得られた知見 93
2. 今後の課題 94
3. 結論 95

謝辞 **97**

研究業績 **99**

参考文献 **101**

図 目 次

2.1 緊急通報型 10
2.2 安否連絡型 11
2.3 安否登録・検索型 12
2.4 情報取得・提供型 (分散提供) 13
2.5 情報取得・提供型 (集中提供) 14
2.6 ライフライン通信の共通基盤モデル 15

4.1 インターネット上での接続先解決 34
4.2 地理的位置情報証明書の発行 38
4.3 地理的位置情報証明書の検証 39
4.4 地理的位置情報証明書と GPS 情報の関係 40
4.5 ユーザ情報証明書の発行 42
4.6 ユーザ情報証明書の検証 43

5.1 ライフライン通信システム 46
5.2 発信側端末画面 49
5.3 着信側の端末画面 56
5.4 地理的位置情報証明書の検証 57
5.5 ユーザ情報証明書の検証 59
5.6 地理的位置情報証明書をとりまく関係図 61
5.7 ユーザ情報証明書をとりまく関係図 62

6.1 システム処理性能 74

表 目 次

2.1 各ライフライン通信型における要件 15

5.1 接続先候補の設定例 67

6.1 鍵長に対する証明書取り扱いの所要時間 72
6.2 データ長に対する証明書取り扱いの所要時間 73
6.3 ラインライン通信における処理時間解析 75

第1章　序論

本章では、インターネットにおけるライフライン通信の実現の重要性、ならびに、その意味と意義をを述べるとともに、本研究の対象、および、取り組みと位置づけを示し、最後に、本論文の構成について述べる。

1. インターネットにおけるライフライン通信

1.1 インターネット上での実現

近年、インターネット接続環境の普及が進み、家庭などでも安価に ADSL や FTTH による広帯域な常時接続環境が利用可能になっているとともに、街角などでも公衆無線 LAN 接続環境などによるインターネット接続が徐々に広まりつつある。このような中、電話を始めとして既存のメディア上で行なわれていた様々な通信がインターネット上へと移行しつつあり、インターネットの重要性が増すとともに、それに応じて、インターネットを緊急通報などのライフライン通信の手段として用いることの重要性も増大しつつある。

1.2 ライフライン通信の意味

ライフライン通信の意味するものとして、地震、台風、テロといった大災害発生時における様々な情報入手・提供や安否情報の通知・登録検索といった意味合いから、日常生活においての警察や消防への緊急通報、あるいは、電気・ガス・水道といった社会的なライフラインサービス提供機関への緊急連絡といったものまで挙げられる。本研究においては、これらの被災状態あるいは緊急事態にある人々に必要とされる通信をライフライン通信として位置付ける。様々な形態の通

信が該当するが、第 2 章においてライフライン通信の分類を示す。

1.3 インターネット上での実現の意義

インターネット上でこのようなライフライン通信をサポートする意義は二つある。一つは、既存のメディアと同様の機能をインターネット上で実現することで、インターネット到達性さえあれば代替として機能するということである。もう一つは、高度なマルチメディア環境のサポートといったインターネットの特徴を生かすことである。それによって、より利便性の高いライフライン通信サービスを提供するだけでなく、子供・老人・障碍者といった人々にも役立つ。

逆に、それらの実現のためには、文字・音声・映像などの多様なメディアに加えて、地理的位置情報・時刻情報・認証情報といった情報のやりとりを行なう必要がある。また、逆に、インターネットへのアクセスさえ可能な環境であれば、人命や災害に関わるライフライン通信を行なうことができるべきであり、状況に応じてインターネット上の様々な通信手段を利用できることが望ましい。

2. 本研究の取り組みと位置づけ

この節では、本研究が対象とする課題と通信環境と通信形態をまず示し、それに対する本研究の取り組みと、本研究位置づけについて述べる。

2.1 本研究の対象

本研究の対象としては、前節で述べたようなライフライン通信を、インターネットのみを利用して実現することを目標とし、その際に必要となるライフライン通信の基盤機能として、通信接続先の解決や発信側のユーザ情報と地理的位置情報の取り扱いについての枠組みを確立する。通信環境としては、発信側も着信側もインターネットに接続して、特に IPv6 にて原則としてエンドツーエンドの通信を想定し、利用者は自分の端末を持ち歩いて異なる場所にて用いることも対象と

する。通信対象としては、音声だけでなく文字や映像など多様なメディアによる通信や、地理的位置情報やユーザ情報など種々の情報の伝達まで幅広く考慮するとともに、メールやウェブといった様々な通信形態についても考慮して、それらにおいて用いることができるような共通の基盤技術の確立を目指す。

なお、本研究の対象は、インターネットにおけるライフライン通信であるため、インターネット接続自体を災害時でもどのように確保し続けるかといった問題、回線や機器設備などの物理的な障害への対策、電源の確保といった問題は、本研究においては対象としない。

また、特定の接続トポロジーを構成することで、その環境においてライフライン通信を確保するというアプローチよりも、インターネット環境さえあればインターネットだけを用いてライフライン通信を完結させることができることを目指し、任意の接続トポロジーの環境においてライフライン通信を行なうことができることを研究対象とする。

2.2 本研究の取り組み

本研究では、まず、ライフライン通信にどういう形態のものがあるかを四つの種類に分類するとともにそれぞれ必要とされる機能を示し、既存メディアとインターネットの違いを中心に、従来より実現されている機能をインターネット上で実現する際に必要となる課題として、通信接続先の解決と発信側のユーザ情報ならび地理的位置情報の取り扱いの問題を示す。また、それらが既存のシステムや技術では解決できていない点を明らかにし、解決実現のためのそれぞれの要求事項を明確にする。

次に、それらの要求事項を満たすものとして、地理的位置情報ベースの ENUM 方式、地理的位置情報証明書方式、ユーザ情報証明書方式を本研究にて提案した。また、それらを元にして構成したライフライン通信システムの実装構築をし、実証実験による動作確認と性能測定を行なう。そして、性能評価、性質評価、他方式との比較評価を行ない、本提案システムが有効であることを示す。

2.3 本研究の位置づけ

本研究では、インターネットにおけるライフライン通信の実現にあたっての、必要となる機能、既存技術での問題、解決するための要求事項を、新たに整理して示している。また、その要求事項を満たす提案方式とそれによるライフライン通信システムを構築をし、実用的に利用可能なことを示している。これらにより、本研究は、インターネット上でライフライン通信を実現するために必要な基盤技術の確立となるとともに、今後の更なる研究のために大きく寄与するものと考える。

3. 本論文の構成

まずは、第1章において、序論としてインターネットにおけるライフライン通信の実現の必要性と、本研究における取り組みと位置づけについて述べた。次に、第2章において、ライフライン通信における課題、インターネットと既存メディアについての違い、関連する既存技術とシステムについて述べる。第3章においては、ライフライン通信の実現の解決のために必要となる要求事項について議論する。第4章においては、その要求事項を満たす新たな提案方式について述べる。第5章においては、その提案方式に基づくライフライン通信システムについて解説する。第6章においては、本提案システムの性能評価と性質評価、および、本提案システムと他の方式との比較評価について論じる。最後に、第7章において、本研究の総括を述べる。

第2章　ライフライン通信とインターネット

ここでは、本研究において対象とするライフライン通信について述べる。既存のメディアとインターネットの違いを論じたあと、インターネットにおいて関連する既存システムとその問題点について述べる。

1. ライフライン通信の種類

前章で述べたように、被災状態あるいは緊急事態にある人々に必要とされる通信であるライフライン通信には、様々な形態が存在する。この節では、ライフライン通信の種類として、緊急通報型、安否連絡型、安否登録・検索型、情報取得・提供型の四つに分類し、次節以降において、それぞれで必要とされる共通基盤機能の要件について示す。

1.1 緊急通報型

ここでの緊急通報型とは、一般利用者からの、警察や消防への緊急通報、あるいは、電気・ガス・水道といった社会的なライフラインサービス提供機関への緊急連絡といったライフライン通信が該当する。特徴としては、着信側がこれらのライフラインサービス提供機関であるとともに、それぞれの機関は地理的に管轄範囲をもって細かく管轄部署が別れている。そのため、発信者の居る場所に依存して、最寄りの適切な管轄部署へと通信が行なわれる必要がある。この緊急通報型で必要とされる機能については、第 2.1 節において述べる。

1.2 安否連絡型

ここでの安否連絡型とは、一般利用者から自分の安否情報などを連絡したい相手へ通信する形態のライフライン通信を指す。緊急通報型とは異なり、発信者の居る場所に依存して通信接続先が変わるわけではなく、それぞれの安否連絡において、発信側が通信したい相手先は明示的に指定される。この安否連絡型で必要とされる機能については、第 2.2 節において述べる。

1.3 安否登録・検索型

ここでの安否登録・検索型とは、携帯電話会社が提供している災害用伝言板サービスや IAA (I Am Alive) システム [6] のように、被災者が現在の安否状況やコメントなどの安否情報を用意された巨大なデータベースへと、登録あるいは検索できる形態のライフライン通信を指す。この安否登録・検索型で必要とされる機能については、第 2.3 節において述べる。

1.4 情報取得・提供型

ここでの情報取得・提供型とは、災害情報などの周知に用いられるライフライン通信を指す。すなわち、被災者などの側から見るとそれらの情報の取得であり、情報をまとめて発信する側から見るとそれらの情報の提供となる。例えば既存のものとして、テレビやラジオなどによる放送がある。また、インターネットにおいては、ウェブ上での災害情報提供などが使われている。この情報取得・提供型で必要とされる機能については、第 2.4 節において述べる。

2. ライフライン通信で必要とされる機能

2.1 緊急通報型

前節で分類した各ライフライン通信の型について、インターネットにおいて実現をする際に必要とされる機能をこの節以降で述べる。まず、緊急通報型について、従来より用いられているメディアとして既存電話網である PSTN (Public Switched Telephone Network) における状況と、必要とされている機能について述べる。

2.1.1 適切な通報先への接続

警察や消防などへのライフライン通信は、どこにいても 110 番や 119 番といった簡易な指定のみで、発信者の居場所を管轄とする最寄りの各署などへ、自動的に接続して通信できる必要がある。

PSTN においては、日本全国どこからでも 3 桁の電話番号をダイヤルするだけで、最寄りの警察 (110 番)、消防 (119 番)、海上保安 (118 番) といった緊急通報受理機関のその地域を管轄する本部の指令台へと接続される。例えば、警察の場合は都道府県単位の管轄となっていて、消防の場合は全国に約 900 の消防本部があり管轄が分かれている。

しかし、PSTN で実現しているこの機能をインターネット上で実現するには様々な課題を抱えている。そこで、インターネット上における通信接続先解決に関する研究が必要である。

2.1.2 発信者の特定識別

ライフライン通信においては、特に、いたずらの抑制やなりすましの防止をするために、発信者あるいは発信端末の識別特定が必要である。また、発信者あるいは発信端末への呼び返しを実現するために、発信者側の情報を正しく把握できる必要がある。

PSTN においては、発信者の電話番号通知機能とともに、発信者側と緊急通報

受理機関との間に接続された通話回線を、発信者側による切断にも関わらず、緊急通報受理機関側から切断するまではその通話回線を保持する、回線保留という機能を持っている。また、回線保留ができない場合、あるいは、完全に切断したあとでも、緊急通報受理機関側が発信者側の電話番号を把握することで、その電話番号に対し呼び返しを行なうことができる。このように、確立された通話回線、あるいは、通知された電話番号によって、発信者側の特定識別を行なっている。

インターネットにおいては、発信者あるいは発信端末のユーザアドレスなどの情報を詐称なく適切に把握することができれば、発信者側の特定識別を実現することができ、いたずらやなりすましの防止と発信者への呼び返しを実現することができる。したがって、ライフライン通信における、発信者のユーザ情報の取り扱いに関する研究が必要である。

2.1.3 発信者の位置情報の通知

ライフライン通信を受けた警察や消防などが、緊急対応を行なったり現場へ駆け付けたりするためには、発信者の居場所である位置情報を正しく把握できる必要がある。

PSTN においては、緊急通報受理機関側は発信者の電話番号を元に加入者情報データベースを検索することで、発信者の住所を把握することができ、これにより位置特定を行なっている。携帯電話においては、加入者情報による住所では意味がないため、複数の基地局による三角測量での地理的位置測定や、携帯電話端末に付いている GPS 機能などで、可能な範囲にて居場所を把握している。

インターネット上においてこのような住所や居場所といった地理的位置情報を扱うためには様々な課題がある。そこで、発信者の地理的位置情報の取扱いに関する研究が必要である。

2.1.4 優先取扱いによる通信品質確保

ライフライン通信は、その利用メディアや通信手段あるいは利用要求に応じて、適切な通信品質が確保される必要がある。それは、ライフライン通信を一般通信

よりも重要であると位置付けて、優先的に取り扱うことにより、利用帯域などの確保や保証を行なうこととなる。

PSTN においては、非常時などに輻輳が発生する場合には、一般通話を制限して、緊急通報を含む重要通信を優先的に接続する機能が備えられている。PSTN は、音声だけを扱うとともに回線交換型であるため、接続されればそのまま帯域確保の意味で通信品質が確保される。

インターネット上でのライフライン通信に関する本研究においては、この優先取扱いによる通信品質確保についての課題を対象としない。以下に、その対象としない理由と、本研究における代替アプローチについて述べる。

本研究の目的は、インターネットが利用できる環境さえあれば、多様なメディアや様々な通信手段を用いて、どこからでもライフライン通信ができるようにするということを掲げている。一般的なインターネット環境では、様々な特性のトラフィックが混在して流れており、この中で優先的な取扱いをして通信品質を確保するには、複雑な帯域資源の確保と制御による運用が不可欠である。そして、接続トポロジーの変更といった困難な仮定をしなければ、バックボーンや IX(Internet Exchange) などにおいても複雑な運用が必要となる。また、無線区間や ADSL などのアクセス区間での帯域資源確保といったことも必要となってくる。これらに対する研究と技術開発は非常に重要であるが、すぐには解決できないと思われる多くの大きな問題を抱えているため、本研究では対象としないこととした。

その代わり、次のような代替アプローチをとることができるように、本研究においては進めている。まず、音声だけではなく映像や文字など含めて特定のものに依存することなく設計することで、仮に通信帯域を十分に確保できないような状況においても、音声通話がだめなら文字会話による通信や、映像がだめなら静止画による通信など、通信帯域が少なくて済む方法を取ることができるようにする。また、リアルタイムコミュニケーションだけでなく、メールやウェブなどの利用も対象とすることで、例えば、通常の文字メールや音声メールなど、連続的に固定帯域が確保できなくても連絡できる手段も利用することができるようする。さらに、発信者のユーザ情報や地理的位置情報などを確実に通知できるように取り扱うことで、例えば、どこにいる誰から緊急通報があった、ということだけで

も通信相手に伝えられるようにする枠組みとする。

2.1.5 対応すべき機能のまとめ

以上をまとめると、緊急通報型のライフライン通信においては、図 2.1 のように、自分の居場所に依存した接続先解決の機能と、自分の居場所である位置情報を通知する機能と、自分のユーザ情報を通知する機能が必要となる。なお、接続確立後のコミュニケーションには様々な場合があり、例えば、双方向で文字や音声や映像などのリアルタイムコミュニケーションを行なう場合や、片方向にメールやインスタントメッセージを送付する場合や、ウェブによるインタラクティブな通信を行なう場合や、なにもなしで位置情報通知とユーザ情報通知のみ自動的に行なわれるような緊急状況の場合などが考えられる。ただし、それぞれのコミュニケーション方法はライフライン通信に限らず用いられる汎用的なものであるため、ここでは各個別の方法には立ち入らないこととし、ライフライン通信に固有で不可欠な、接続先解決と位置情報通知とユーザ情報通知に焦点を当てる。

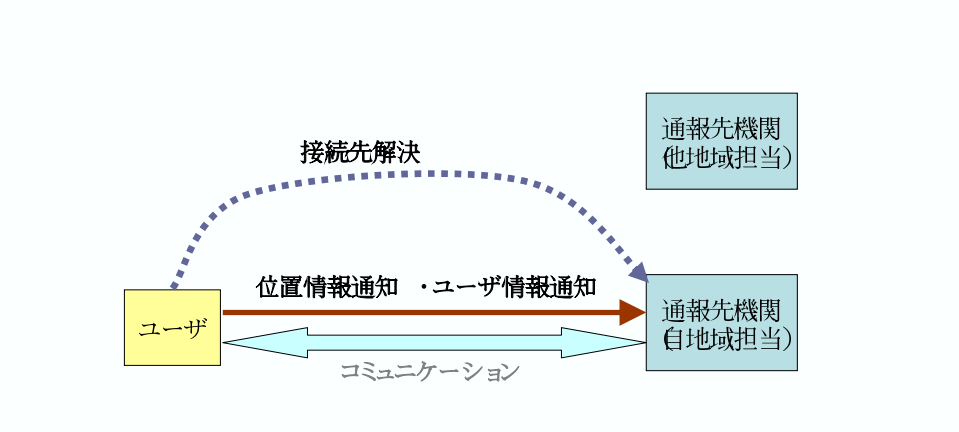

図 2.1 緊急通報型

2.2 安否連絡型

安否連絡型は、一般利用者から自分の安否情報などを連絡したい相手へ通信する形態のライフライン通信であるが、緊急通報型とは異なり、発信側が通信したい相手先は一意に確定している。しかし、安否連絡のための機能として、位置情報通知とユーザ情報通知の機能は、緊急通報型と同様に必要となる。また、接続確立後のコミュニケーションについても同様であり、図 2.2 のように緊急通報型から接続先解決の機能を除いたものと同じ形態となる。

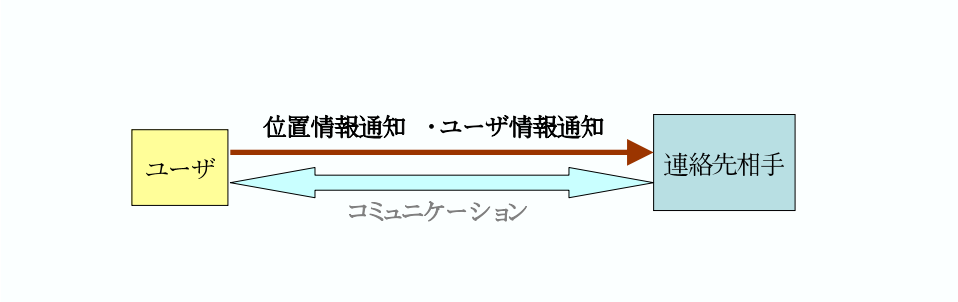

図 2.2　安否連絡型

2.3 安否登録・検索型

安否登録・検索型のライフライン通信は、IAA システムに代表されるように、安否情報の登録機能と安否情報の検索機能を中心に構成される。その他に、データベースシステム内での情報の管理やクラスタ化などもシステムの重要な要素であるが、各個別システムの内部の話となるためここでは扱わない。

一方、例えば、IAA システムにおける登録においては、入力情報は完全に自己申告となっており、本当に本人が登録したのかどうかを確認することができない。しかし、入力情報のうち、位置情報とユーザ情報は、緊急通報型や安否連絡型と同様に重要な要素であり、これらの情報はユーザが意識することなくシステムへと通知されるとともに、システム側でもその情報の正当性が確認できることが望ましい。

また、地域的に分散してサーバなどが設けられている場合、最寄りのサーバを利用できることが望ましい。この場合は、緊急通報型と同様に、接続先解決の機能が必要となる。これらをまとめると、図 2.3 となる。

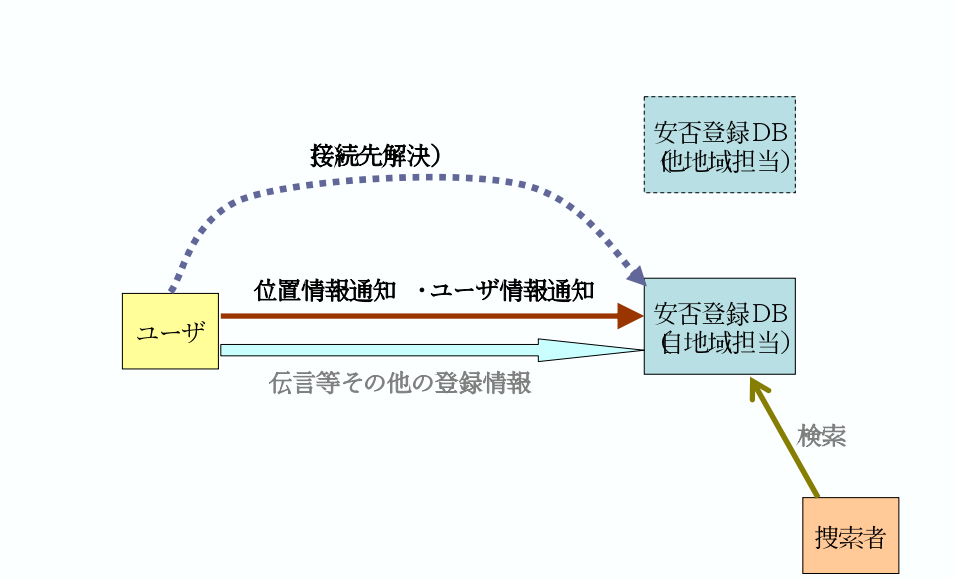

図 2.3 安否登録・検索型

2.4 情報取得・提供型

災害情報などの周知に用いられるライフライン通信である情報取得・提供型は、従来はテレビやラジオ放送を中心として行なわれてきた。一方、インターネット上においては、テレビやラジオと同様にストリーム放送を行なうこともできるが、それに加えて、ウェブ上での災害情報提供による周知も行なうことができる。

2.4.1 適切な情報取得先への接続

インターネット上では広域ブロードキャストは存在せず、ストリーム放送による情報提供の場合でも、IP マルチキャストによる放送の受信か、サーバへの接続を行ないユニキャストによる放送の受信をする必要がある。IP マルチキャストの

場合、情報を取得したい端末はどのマルチキャストグループなのかを解決して、そこへと受信参加 (JOIN) することで、実際に受信をしてストリーム放送で提供されている情報を受信することができる。また、ユニキャストによる放送受信の場合も、どのサーバへと接続すればいいかを解決して、そこへ接続することで、情報を受信することができる。一方、ウェブ上提供されている情報を取得する場合も、どのウェブサーバへと接続すればいいかを解決して、そこへ接続することで、情報を取得することができる。

このように、どのタイプであっても、まずは接続する先を解決する必要がある。これらの提供される情報は各地域毎に異なり、対応して接続先も異なる。つまり、各地域毎にその地域の情報を提供するサーバが個別に存在することが多いためである。さらに、提供される情報の種類によっても、対応して接続先も異なることもある。このような状況のもとで、例えば、旅先における見知らぬ地域において災害情報提供を取得したいとすると、そのユーザは最大でも情報の種類を指定する程度で、自分が今どこにいるかを意識せずに接続できるのが好ましい。この点では、緊急通報型における接続先解決と同じものが求められる。この通信形態を表したものが、図 2.4 である。

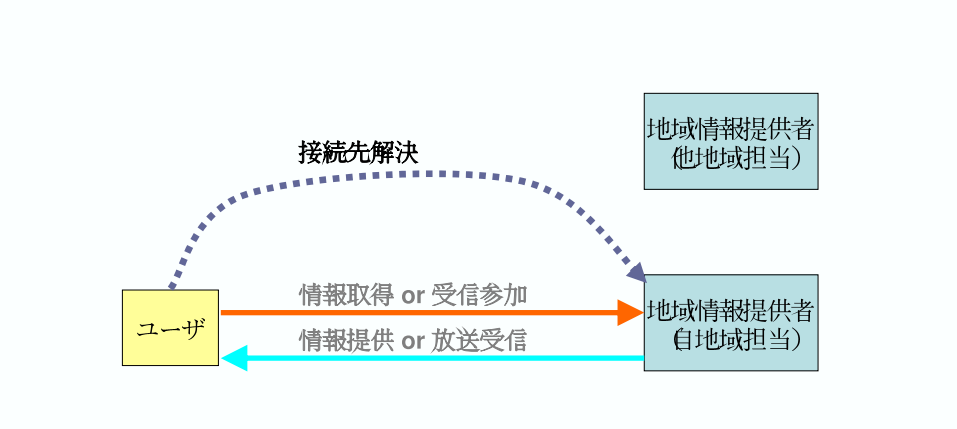

図 2.4 情報取得・提供型 (分散提供)

2.4.2 発信者の位置情報の通知

一方、ウェブサーバなどによる情報提供において、各地域毎にその地域の情報を提供する方式だけでなく、例えば全国の情報を一つのサーバで提供している場合も多い。このような場合、ユーザは自分の位置情報をサーバに伝えることで、指定された位置を含む地域の情報を得るといった利用方法も試みられている。この場合は、図 2.5 のように、位置情報通知の機能が必要であり、すなわち、緊急通報型などの場合と同様に、ユーザが意識せずに自分の居場所の位置情報を得るとともに、必要に応じて自動的に通知する機能が必要となる。

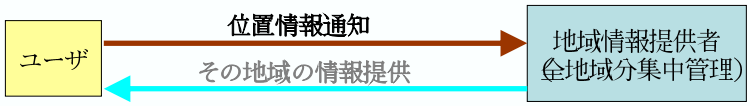

図 2.5 情報取得・提供型 (集中提供)

2.5 ライフライン通信で必要とされる機能

以上の四つのライフライン通信の分類において、それぞれにおける要件をまとめると、表 2.1 となる。このように、接続先解決と位置情報通知とユーザ情報通知の機能は、様々なライフライン通信の形態を越えた共通に必要とされる機能である。特に、緊急通報型のライフライン通信は三つの要件を全て含んでいる。

以上の議論により、本研究においては、ライフライン通信を接続確立するために必要な固有の機能の課題として、図 2.6 のように、インターネット上での接続先解決、発信者の地理的位置情報の取扱い、発信者のユーザ情報の取扱い、の三つの課題を対象とする。本研究では、これらのライフライン通信における共通基盤技術の確立を目指す。

表 2.1 各ライフライン通信型における要件

	接続先解決	位置情報通知	ユーザ情報通知
緊急通報型	○	○	○
安否連絡型	—	○	○
安否登録・検索型	△	○	○
情報取得・提供型 (分散提供)	○	—	—
情報取得・提供型 (集中提供)	—	○	—

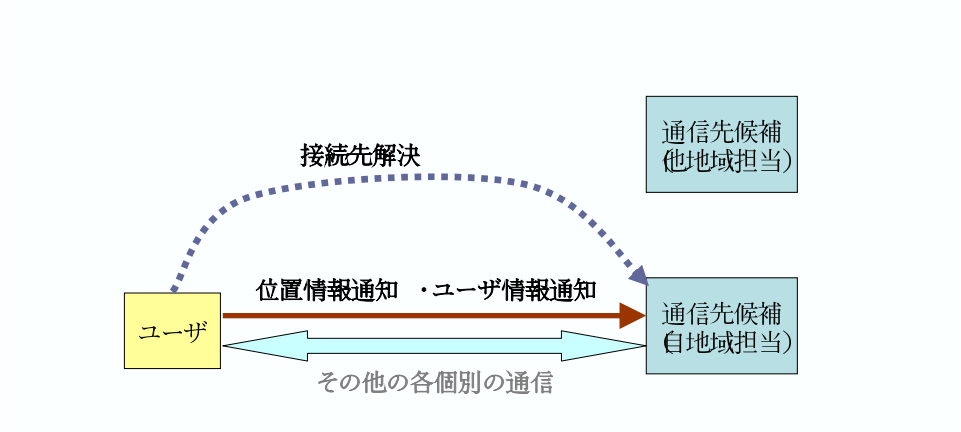

図 2.6 ライフライン通信の共通基盤モデル

3. インターネットとPSTN

PSTNとインターネットの間の様々な違いによって、既存のシステムをそのままの形、あるいは、そのままの概念でインターネットへ導入することは困難である。インターネットとPSTNは非常に多くの点で異なり、PSTNにおいて実現できているライフライン通信の機能をインターネットにおいても実現するには、その違いを理解しておく必要がある。ここでは、インターネットとPSTNについて、その機能と違いについて述べる。

3.1 ネットワークと端末の位置付け

インターネットとPSTNの違いとして、ネットワーク側と端末側のどちらにインテリジェンスがあるかということが挙げられる。PSTNにおいては、ネットワーク側がインテリジェントであり、その中心である交換機が様々なルーティング機能や様々な情報のやりとりの扱いを管理する。そして、電話端末は制限された単純な機能だけを持つ。一方、インターネットにおいては、ネットワーク側にあるルータは基本的にはパケット転送機能だけを受け持つ。そして逆に、IP端末側において様々な複雑な機能を実現している。さらに、PSTNはネットワーク側によって管理された回線交換に基づいており、一方、インターネットはパケット交換に基づいており、さらに、ネットワーク側では必要最小限の経路情報しか管理しない。

3.2 識別子とルーティング

呼やパケット等のルーティングにおいて、PSTNでは、交換機が電話番号に基づいてルーティングを行なう。一方、インターネットでは、ルータがIPアドレスに基づいてルーティングを行なう。例えば、インターネットにおいて電話番号に基づいてルーティングするためにIPパケット中のIPヘッダ等に電話番号を格納したとしても、ルータにはそれを理解して処理する機能はなく、さらにルータが各電話番号への経路表を持つのは効率がよくない。また、それらの機能を新たに

ルータ製品に組み込んで普及させるのも現実的ではない。したがって、インターネットにおいては、与えられた電話番号に対応する接続先の IP アドレスをなんらかの形で解決してから通信をする必要がある。

3.3 インターネットにおける識別子

インターネットにおける識別子として、上記に挙げたルーティングのための IP アドレスに加えて、ドメイン名およびユーザアドレスが存在する。ドメイン名は、example.jp や host1.example.jp といったように、そのドメイン名が与えられた組織あるいは属するホストなどを示すために用いられる識別子である。これらは DNS[8] によって、IP アドレスと対応関連付けることができ、IP アドレスよりも抽象度の高い識別子として使われている。

ユーザアドレスはさらに抽象度の高い識別子であり、user@example.jp といったようにユーザ@ドメインの形式をとる。これは、メールアドレスや SIP アドレス [9] などでも用いられている。あるホスト上のあるユーザを userA@host1.example.jp として示せるだけでなく、userA@example.jp という形で特定のホストを指定せずにドメイン名のみを指定し、ユーザを抽象的に表現する形で用いることも多い。インターネット上においては、このようなユーザアドレスを用いることで、ユーザの識別や指定が行なわれている。

汎用的には、インターネット上のリソースを指し示すものとして、いわゆる URI (Uniform Resource Identifier) 形式 [10] をとるインターネットアドレスがあり、通常この中には通信プロトコルの指定まで含まれている。例えば、インターネット電話で用いる SIP アドレス sip:user@example.jp や、メールアドレス mailto:user@example.jp といったユーザアドレスに対して通信プロトコル指定が付加されたものや、ウェブアドレス http://www.example.jp/や、FTP アドレス ftp://ftp.example.jp/などが挙げられる。これらのうち、ユーザを指し示すメールアドレスや SIP アドレスなどについても、ユーザアドレスと呼ばれて、インターネット上でのユーザに対する識別子として用いられる。

これらのインターネットアドレスが与えられた時も、実際にインターネット上で通信を行なうことができるためは、通信接続先の IP アドレスを解決できる必

要がある。ウェブアドレスや FTP アドレスの場合は、指定されているホスト名に対応する IP アドレスを DNS にて解決できる。また、メールアドレスや SIP アドレスの場合は、それぞれのユーザ@ドメイン部におけるドメイン部分に対し、各プロトコル毎に定められた規則にて DNS を検索することで、通信接続先の IP アドレスを解決できる [11]。

3.4 管理把握体制の違い

PSTN とインターネットのそれぞれのサービス提供者である、電話会社と ISP (Internet Service Provider) の役割も大きく異なる。PSTN においては、各端末は電話会社の交換機や基地局などに直結しており、各端末のおおよその地理的な位置情報を、加入者情報や基地局の位置などによって、電話会社はおよその地理的位置を把握できている。しかし、インターネットにおいては、個人や組織が ISP から IP アドレス空間を割り当ててもらうことができ、それを用いて自由に自分のネットワークを構築することができる。よって、その IP アドレス空間を割り当てた ISP であっても、必ずしも各端末がどこにあるかを知ることはできない。

また、個人や組織は、IP アドレス空間を割り当ててもらった ISP に依存することなく、自分達の独自のドメイン名を取得して利用することができる。そして、そのドメイン名を用いて、ウェブサーバやメールサーバあるいは SIP サーバなどを運用することができ、それらに基づく、ウェブアドレスやメールアドレスあるいは SIP アドレスが、インターネット上での識別子として一般的に使われている。

4. 既存技術と問題点

ここでは、インターネットにおいて関連する既存技術とその問題点について述べる。

4.1 ENUMによる接続先解決

前節で示したように、インターネットにおいて、電話番号をそのまま用いてIPパケットをルーティングすることはできない。そこで、電話番号に対応する接続先のIPアドレス、あるいは、IPアドレスへ解決可能なインターネットアドレス(URI)へと、電話番号から変換をしてからIP通信を行なう必要がある。ENUM (Telephone Number Mapping) [12] は、そのように電話番号をインターネット上のサービスに対応させる枠組みの技術である。現在、IETF(Internet Engineering Task Force)とITU-T(International Telecommunication Union Telecommunication sector)が協調してENUMの国際標準化を進めている。

ENUMを用いて電話番号からインターネット上の接続先を解決しようとする利用者は、与えられた電話番号を国番号付のE.164形式 [13] をもって検索キーとし、DDDS (Dynamic Delegation Discovery System) [14] という汎用的な枠組みを使ってDNSのNAPTRレコードを検索することで、その電話番号に対応するインターネットアドレスのリストを得ることができる。結果のリストとして得られるものは、メールアドレス・ウェブアドレス・SIPアドレスなど様々な通信手段によるインターネットアドレスである。また、負荷分散、あるいは、バックアップなどのために更にそれぞれが複数候補リストとなっている場合もある。

このように、インターネット上で電話番号に対してその接続先を解決する枠組みは、世界標準として現在進められつつある状況にある。しかし、残念ながら、日本における110番や119番などのような特番については、ENUMの対象外とされている。なぜなら、それらの特番は各国によって割り当て事情が異なるというだけでなく、発信者がどこの地域にいるかに依存して、解決されるべき接続先が異なるためである。

一方、特番を持たないライフライン通信、例えば、ガス漏れ・水道漏れ・電気漏れなどの緊急通報先の電話番号などは、日本では一般電話番号が使用されているため、ENUMを用いて、対応するインターネットアドレスへと解決することができる。しかし、地域によってその電話番号自体が異なるため、まず先にその電話番号自体を把握しておかなければ利用することができず、簡易なアクセス方法によるライフライン通信の実現、といったユーザの利便性の面を満たすことがで

きていない。

4.2 HTTP/SIP ヘッダによる位置情報通知

インターネットにおける地理的位置情報の扱いの一つとして、HTTP ヘッダを拡張してウェブサーバへ地理的位置情報を伝える試み [15] がある。これの枠組みを、例えばウェブベースの緊急通報受け付けや、ウェブベースの安否情報の伝言板システムなどに利用することは可能である。

しかし、この方法では、ユーザから自己申告された地理的位置情報を、受理した側はそのまま信頼するだけのものとなってしまい、地理的位置情報に対する詐称などを防ぐことができない。

4.3 位置情報登録管理システム

インターネットにおいて地理的位置情報を取り扱うシステムとして、GLI System [17][18] がある。これはインターネット上で移動体の地理的位置情報を管理するシステムであり、ユーザからの地理的位置情報の登録や検索をサポートしている。このシステムを用いることで、ユーザは自分の地理的位置情報を登録しておき、例えば緊急通報の場合に警察や消防などのライフラインサービス機関側は、発信者の地理的位置情報を検索するといったことが可能である。

しかし、この方法では、ユーザから自己申告された地理的位置情報を、受理した側はそのまま信頼するだけのものとなってしまい、地理的位置情報に対する詐称などを防ぐことができない点と、通信相手側からの検索におけるユーザの識別という点で問題がある。

4.4 DHCP による位置情報提供

ネットワーク側から地理的位置情報を提供するしくみとして、DHCP[19] を利用するものが、提案されている [20][21]。しかし、この DHCP を利用するものは、DHCP から得た地理的位置情報を通信相手へ伝達したときに、その通信相手は自

己申告された情報と区別をつけることができないといった問題がある。

4.5 DNS による位置情報登録と提供

ネットワーク側から地理的位置情報を提供するしくみ、あるいは、登録するしくみとして、DNS を利用するものが、提案されている [22][23]。これによって、ユーザ自身が自分の地理的位置情報を得たり、あるいは、通信相手が発信者の地理的位置情報を得たりすることが可能である。

しかし、これらの DNS を利用する方式は、プライバシーに関する問題がある。DNS へのアクセスは、一般にアクセス制御が行なわれないとともに、アクセス制御も困難でもあり、アクセス制御をしなければ、誰もが登録された地理的位置情報を入手することができてしまう。

第3章　ライフライン通信のための要求事項

この章では、ライフライン通信のために解決すべき課題である、インターネット上でのライフライン通信の接続先解決、発信者の地理的位置情報の取扱い、発信者のユーザ情報の取扱い、それぞれについて議論を行ない、要求事項を整理する。

1. ライフライン通信の接続先解決

まずは、ライフライン通信をインターネット上で実現するための要求課題のうち、接続先解決の問題について述べる。

1.1 特番と一般電話番号

ライフライン通信においては、利用者は意識することなく最寄りの適切な機関へと通信できる必要がある。既存の PSTN においては、日本における 110 番や米国における 911 番のような特番が存在し、利用者はその特番へコールするだけで、適切な接続先と通信することができる。日本においては、警察は 110 番、消防と救急は 119 番となっているが、米国では区別なく 911 番であり、消防と救急が別れているケースもあれば、ガスに関する緊急通報が特番を持っているケースもあるなど、各国によって特番の個数や番号や種類分けは多種多様に異なっている。

一方、すべてのライフライン通信が特番を持つわけではない。日本においては、電気・ガス・水道などの生活ライフライン系に対する緊急通報は、特番ではなく一般電話番号が使われている。そのため、これらの特番を持たないラインライン通信サービスそれぞれについて、各地域に応じて定まる一般電話番号を、利用者

は覚えたりメモしたりしておく必要があり、利用しにくいのが実情である。したがって、ユーザにとって簡易なアクセスで利用しやすいことも求められる。

1.2 インターネット上でのサービス

PSTN においては基本的に音声による通報のみであるが、インターネット上では、音声などのリアルタイムコミュニケーション型だけではなく、メールやウェブなど様々な手段によるライフライン通信がサポートされつつある。例えば、電子メール 110 番などをサービスとして導入しているところは既に多い。さらに、ウェブによる文字対話方式による緊急通報受付サービスを導入しているところも存在する。そして、今後は TV 電話の形態などを含むインターネット上の様々な通信手段によって、ライフライン通信サービスがサポートされていくものと予想される。したがって、それらの様々な通信手段をすべて考慮しておくことが必要である。

しかし、これらのサービスで用いられているメールアドレスやウェブアドレスは、各地域によって全く異なりばらばらの形式であるなど、実際の利用にあたっては、それぞれのインターネットアドレスを個別に覚えたり、アドレス帳などに自分で登録したりせねばならない。さらに、旅行などで移動して別の地域にいる時は、その地域に対応するアドレスを調べて、ユーザが意識して切り替えて指定して利用せねばならない。例えば、電子メール 110 番などは各県警によってメールアドレスは異なっている。このように、ユーザにとって簡易な指定ですむ状況にはなっていない。

したがって、これらを含む様々な機関へのライフライン通信に対して、利用者がどのライフライン通信サービスを利用したいのか種別を単に指定するだけで、自動的に適切な接続先のインターネットアドレスが得て、それを利用することができることが求められる。例えば、利用者がいちいち各県でのメールアドレスを覚えていなくても、ライフラインサービスの種類として警察を指定するだけで、利用者は個別のインターネットアドレスを意識することなく、通信することができるような簡便さが求められる。

1.3 サービスによる管轄地域区分の違い

これらのライフラインサービスは、各サービス毎に個別の異なる管轄担当区域を持っている。そして、ユーザからの緊急通報呼び出しによって、その地域を管轄する機関へと適切に接続される必要がある。例えば日本において、警察は都道府県単位の管轄であり、消防・救急は市町村あるいは市町村の連合などによる地域単位の管轄が行なわれていて全国で約 900 カ所の消防本部へと適切に接続される必要がある。また、水道サービスは市町村単位であったり一部地域は県営であったりと、地域により異なる管轄方法をとっている。ただし、どのライフラインサービスにおいても、自分のいる地域がどこであるかが決まれば、その居場所がどこであるかの情報だけに依存して、そこを管轄とする通信接続先が確定する。

例えば既存の電話では、各サービスにおいて自分の居場所の管轄外のところへ電話をしてしまった場合には、そのような管轄外からの通報には地理的な不案内などによって迅速な対応が困難であることが多く、正しい管轄が把握できてからようやく、電話をそこへ転送してもらったり、かけ直すよう指示される結果となる。ライフライン通信においては、そのようなやりとりの時間が非常に貴重であるだけでなく、出かけた先で自分が地理的に不案内である場合や、緊急事態においては正確な受け答えが難しい場合も考えると、発信者が意識することなく正しい接続先と通信できることが望ましい。

このように、各ライフライン通信に関して各機関はそれぞれ各地域を個別に管轄しており、利用者は自分の居る場所をちょうど管轄している部署へ接続して通信する必要がある。自分の地域の管轄外のところへ緊急通報が接続されてしまったとしても、上述したように、多くの場合は緊急対応をすることが困難であるという現状があるため、これらの要求は確実に満たす必要がある。

1.4 接続先解決における要求事項

このように、ライフライン通信においては、発信者は自分がどこにいるかを意識せずに利用できる必要があり、発信者がどこにいるかに依存して、対応する通信接続先が異なる。そして、それらは警察や消防といった各ライフラインサービ

ス毎に、その対応付けが異なる。発信者は、どのライフラインサービスに対して通信をおこなうのかを、簡易な手段で指定するだけで、実現できる必要がある。また、従来の電話と同じ音声による通話だけでなく、文字や映像による通話に加えて、メールやウェブなどインターネット上の多様な通信手段をサポートする必要がある。接続先への通信手段に複数の選択肢がもしあれば、発信者は、どの通信手段を用いるのかを、簡易な手段で指定するだけで、実現できる必要がある。そして、その通信接続先は、発信者の居場所、すなわちどこにいるかに依存して決定されるため、発信者の地理的位置情報を把握できる必要がなる。そして、その地理的位置情報を利用することで、通信接続先を解決できる必要がある。

2. 発信者の地理的位置情報の取扱い

ここでは、ライフライン通信をインターネット上で実現するための要求課題のうち、発信者の地理的位置情報の取扱いの問題について述べる。

2.1 地理的位置情報の必要性

ライフライン通信においては、通信を受けた着信側は、発信者の居場所を把握できる必要がある。なぜなら、発信者の地理的位置情報を得ることで緊急対応を開始することが可能となり、さらに必要であれば発信者の元へと急いで駆け付けることを可能とするためである。したがって、その情報はできる限り正確な情報であることが求められる。また、なりすまし防止やいたずら抑制のため、詐称された情報でないことが保証される必要がある。

また、前節で述べたように、適切な通信相手への接続を行なうためには、発信側においても、発信者の居場所の地理的位置情報が必要となる。したがって、発信側ならびに着信側の両方において、発信者の地理的位置情報を把握できることが求められる。

2.2 地理的位置情報のプライバシー

発信者の居場所を示す地理的位置情報については、通信の秘密やプライバシーの保護の観点から、通知などの際に発信者による意思確認が確実に行なわれるべきものとされており、また、保護されるべき個人情報の一つとして、その取り扱いには十分注意する必要がある。

よって、発信者当人、および、発信者当人がインターネット接続等に用いているネットワークの管理側が自動的におよその位置を把握できることを除き、他者が発信者の地理的位置情報に対して勝手にアクセスすることは基本的に禁じられるべきである。

ライフライン通信の場合には、接続先（緊急通報の場合はライフラインサービス機関、特定の相手への安否通知の場合はその相手など）が、その時点での発信者の地理的位置情報のみを入手できる必要がある。

つまり、たとえライフラインサービス機関であるからといって、通報した発信者以外の地理的位置情報を取得できてはならず、また、発信者の地理的位置情報についても、通報時と無関係の時の居場所情報を取得できてはならない。したがって、それらを満たすようにアクセス制御か、情報の流れの制御が必要となる。

2.3 GPS による地理的位置情報

最近は、GPS 受信機などを用いることで手軽に地理的位置情報を取得できるようになっている。しかし、屋内などをはじめとして利用できない場所や環境も多く、また、全ての端末がそれらの受信装置を備えているわけではないため、常に GPS からの情報を利用できるわけではない。したがって、GPS などによる情報が入手ができない場合でも、ライフライン通信で必要となる発信者の地理的位置情報を、なんらかの形で入手できる必要がある。

しかし、最も重要な問題は、GPS 受信機などから自分の地理的位置情報を入手できている状況においても、得られた自分の地理的位置情報をインターネットを通して他人に伝えたとき、情報を伝えられた相手にとって、その情報は本当に GPS から得られたものなのか、あるいは、情報を詐称しているのかを、区別でき

ないことである。例えば、GPS 受信装置が付いている端末において、GPS 受信装置から得た情報の内容は、その時点でその発信側端末しか知らない。そのため、その発信側端末からインターネットを通して GPS 情報を送付することで初めて、送付を受けた着信端末や代理サーバなどの他の者が、その情報を入手できる。つまり、発信側端末が情報を改変して送付していても、それだけでは詐称を見破ることができない。

この、情報の正当性を確認できない問題は、必ずしも GPS あるいは類似システムから入手した地理的位置情報のみに限定された問題ではない。例えば、地理的位置情報を表示しているバーコードや RFID などから読み取った情報のときも同様であるし、DHCP などによってインターネットから得た地理的位置情報を相手に送付して伝える場合についても、全く同じ問題が生じる。

したがって、GPS などから地理的位置情報が取得できる環境においても、インターネット上でその地理的位置情報の通知などといった取り扱いに関しては、単に送付すればよいといった簡単な状況ではない。ライフライン通信においては、間違った情報、あるいは、詐称された情報が通知された場合に特に深刻であるため、情報の通知を受けた側で、通知された情報の正当性をなんらかの方法で確実に検証できることが求められる。

2.4 地理的位置情報に関する要求事項

このように、ライフライン通信においては、インターネットだけを用いて、発信側では自分自身の地理的位置情報を把握できることが求められる。ライフライン通信を行なってる際には、その接続先の通信相手側において、発信側の地理的位置情報を把握できることが求められる。発信側の地理的位置情報を入手した着信側は、その情報が詐称された情報でないことを検証できることが求められる。本人と接続先ネットワークを除いて、その時にライフライン通信を行なっていない相手は、地理的位置情報を取得できてはいけない。これらは、ライフライン通信で用いる通信手段に依存せずに実現することが求められる。

3. 発信者のユーザ情報の取扱い

ここでは、ライフライン通信をインターネット上で実現するための要求課題のうち、発信者のユーザ情報の取扱いの問題について述べる。

3.1 ユーザ識別子の必要性

ライフライン通信においては、なりすましを防止したり、いたずらを抑止するために、発信者側の情報を把握して識別できる必要がある。また同時に、緊急対応などのためにも、発信者側の情報を正しく把握できることが求められる。また、発信者側への呼び返しができることも求められる。これらを実現するためには、発信者側のユーザ情報の入手把握が必要であり、ユーザ情報のうち、特にユーザ識別子による特定と識別を行なうことで、なりすましやいたずらへの対策となるとともに、発信者への呼び返しも可能となる。

3.2 インターネットにおけるユーザ識別子

前節での説明のように、インターネットにおいては識別子として、IP アドレスやユーザアドレスなどが用いられる。しかし、IP アドレスはユーザ識別子としてはふさわしくない。例えば、ADSL ユーザがライフライン通信をしているときに、なんらかの理由で ADSL が切断されて再び繋がったとすると、必ずしも以前と同じ IP アドレスを割り当ててもらえるとは限らない。また、移動などで別のネットワークへ繋ぎ変われば、当然異なる IP アドレスを割り当ててもらうことになる。そのため、ユーザ識別子として IP アドレスを用いた場合、発信者へ呼び返しをすることができない。

一方、変化しない固定の IP アドレスを使えるようにするしくみとして、モバイル IP が挙げられる。モバイル IP を用いることによって、端末を持ち歩くユーザであっても、行く先々で割り当てられる IP アドレスとは独立に、固定の IP アドレスを利用することができる。しかし、メールを用いる場合には、識別子として IP アドレスを用いるよりも、ユーザ@ドメイン形式であるメールアドレスを

用いた方が便利である。また、VoIP などのリアルタイムコミュニケーションにおいて SIP を用いる場合でも、IP アドレスを指定して通信するよりも SIP アドレスを用いた方が便利である。例えば、その固定の IP アドレスを持たせている端末がその時たまたまインターネットにつながっていない場合に、転送で別のところへ呼び出しを回したり、あるいはユーザが多忙で出られなかった場合に、留守番伝言センターへ回したり、といったことが、抽象的な SIP アドレスであるユーザ@ドメイン形式を用いていれば、呼制御を SIP サーバ経由にできるため、容易に実現できる。それに対し、IP アドレスを用いて直接通信していると利便性が損なわれてしまう。

したがって、ユーザ識別子としては、一般的に使われているメールアドレスや SIP アドレスのようなユーザ@ドメイン形式、すなわち、ユーザアドレスが用いられるべきである。また、この形式を利用することにより、インターネット上での各組織、あるいは、各管轄単位などに割り当てられているドメイン名を元にして、各ユーザがどこに属しているのかが明確となる。

ユーザは複数のドメインに属することができ、各ドメインにおいて異なるユーザアドレスをもらうことができる。例えば、一人のユーザが、複数の異なるドメインにおいて、それぞれメールアドレスをもらって使用しているということは一般的に行なわれている。そして、この場合、ユーザは通信する相手に依存して、自分が用いるユーザアドレスを選択して通信することが可能である。

3.3 ユーザ識別子を付与する対象

これらのユーザ識別子は、人間に対してだけでなく、端末機器などに対しても付与することができる。ここではユーザ識別子の付与対象を、人間、あるいは、端末機器のどちらか片方には限定していない。人間であっても端末機器であっても、それを通信対象とすることができる運用ならば、それぞれが SIP アドレスなどのユーザアドレスを持ち、それをもって通信を行なうため、それを見て特定識別をすることが可能となる。

このような点において、現実面では、人間と端末機器を区別することは非常に困難である。例えば、従来からの電話においても、自宅の電話番号が人間を対象

としているのか端末機器を対象としているのか厳密には難しく、局面によってどちらの見方も可能となる。つまり、契約者は人間であり、その人間に割り当てられている電話番号であるとみなせる一方、実際に利用する人は家族であったり客であったりする可能性があり、識別し割り当てられている対象は、単なる端末機器であるともいえる。この点では、従来の電話においては、自宅の固定電話だけでなく、携帯電話ですら、他人が使いうることを考えると、人間と切り離した形で、端末自体が識別の対象となっているともいえる。

インターネット上における VoIP 端末を利用した通信においても、同様のことがいえる。例えば、あるユーザに割り当てられた SIP アドレスであるユーザ@ドメインについて、ユーザはなんらかの端末機器を介してそれを用いる。このとき、そのドメインの SIP 登録サーバへ SIP 登録の設定を行なう必要があるが、サーバとの認証のためのパスワードを端末機器内に保存して自動登録運用ができるようにしていれば、いくらその SIP アドレスが人間を対象として割り当てられていたとしても、その本人がいなくても使用できてしまう。その点において、識別子としてその SIP アドレスが対象としているものは、人間であるのか端末機器であるのか、変わらなくなってしまう。

もちろん、通信時になんらかの形で必ず本人確認することができる運用をしていれば、確実に人間が識別対象となっているといえるし、逆に、公衆端末のように不特定多数の者が用いることを前提として設置される場合、端末自体に SIP アドレスを与え、サーバへの SIP 登録認証も端末自体が認証を受ける、といった運用も存在する。

これらの運用方法の実態は、外からは知ることは困難であるため、今回はこれらの問題には立ち入らずに、単純に識別対象としてはユーザアドレスを対象とすることにする。ユーザアドレスを含むユーザ情報の中に、もし必要であれば属性として、公衆端末であることを示す情報を含ませるといった方法が考えられる。

3.4 ユーザ識別子の正当性

ライフライン通信においては特に、通知されてきた発信者のユーザアドレスについて、それが正当であるかを検証できる必要がある。つまり、その正当性を検証

することができなければ、本物であるか詐称であるかの判断することができない。

また、正当性が検証された発信者のユーザアドレスに対して、ライフライン通信の場合には、呼び返しが実現できるべきである。つまり、発信者がたしかにそのユーザアドレスを持つ者であるということが判明していたとしても、そのユーザアドレスを用いて、その者への呼び返しをすることができなければ、ライフライン通信としての要件を満たすことができない。したがって、発信者のユーザ識別子であるユーザアドレスは、その正当性が検証されるとともに、呼び返しによって呼び返しをすることができることが保証される必要がある。

3.5 ユーザ情報に関する要求事項

このように、ライフライン通信を行なってる際には、その接続先の通信相手側において、発信側のユーザ情報を把握できることが求められる。発信側のユーザ情報を入手した着信側は、その情報が詐称された情報でないことを検証できることが求められる。また、発信側のユーザ情報を用いて、呼び返しが出来る保証が求められる。本人とそのホームドメインを除いて、その時にライフライン通信を行なっていない相手は、地理的位置情報を取得できてはいけない。これらは、ライフライン通信で用いる通信手段に依存せずに実現することが求められる。

第4章　提案方式

この章では、前章のライフライン通信とインターネットにおいて議論を行なった、ライフライン通信におけるインターネット上での接続先解決、発信者の地理的位置情報の取扱い、発信者のユーザ情報の取扱い、に対して、それぞれにおいて挙げられた要求事項を満たすものとして、地理的位置情報ベースの ENUM 方式、地理的位置情報証明書方式、ユーザ情報証明書方式の三つの方式を提案する。

1. 地理的位置情報ベースの ENUM

ここでは、インターネット上におけるライフライン通信の接続先解決の方法として地理的位置情報ベースの ENUM 方式を提案する。

1.1 ENUM のしくみ

ENUM は、一般の電話番号をその電話番号に対応するインターネット上の接続先アドレス（URI）のリストへマッピングする枠組みを提供するものであり、IETF と ITU-T が協調して国際的な標準として現在議論や実験運用が進められつつある。

図 4.1 の上部に ENUM の概要を示した。国番号を頭につけた E.164 形式の電話番号が与えられたとき、その電話番号を逆順にドットを１つずつはさみ、さらにその後ろ（ドメイン名としては上位）に ENUM 用のドメインである e164.arpa. をつけたものによってドメイン名を構築し、そのドメイン名を DNS 上で NAPTR レコードを検索することで、その電話番号に対応するインターネットアドレスのリストを得る。具体的な例として、図 4.1 では電話番号 +81-743-79-5026 が与えられた

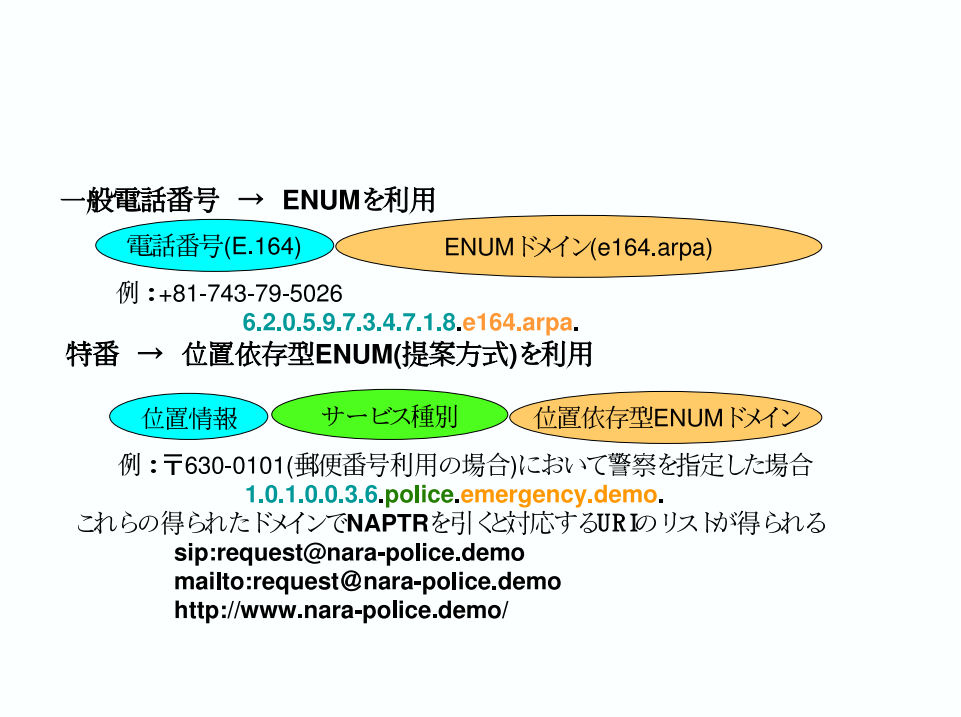

図 4.1 インターネット上での接続先解決

場合を示している。ここから導かれるドメイン名は 6.2.0.5.9.7.3.4.7.1.8.e164.arpa. となる。そして、そのドメイン名の NAPTR レコードを DNS にて引くことで、例えば、図 4.1 の下部にある三つのインターネットアドレス、ここでは SIP アドレスとメールアドレスとウェブアドレスが得られる。

このように、ENUM においては電話番号に対応するインターネットアドレスが得られるので、そのうちの SIP アドレスを用いれば、インターネット上での VoIP 等による接続先が解決できる。また、ユーザは数字だけの電話番号をユーザインタフェースとして指定することで、対応するよう登録されたメールアドレスやウェブアドレスも簡易に利用することができる。

1.2 ENUMの枠組みの応用

ただし、110番や119番といった特番などは、発信者の居る場所によってマッピング先が異なるため、ENUMの対象外となっている。つまり、110番や119番といった特番をこのENUMの枠組みでインターネットアドレスへと対応させようとしても、発信者がどこにいるかに関らず同じインターネットアドレスしか得られないため、このままではENUMの枠組みを利用することができない。

一方、ある地理的位置情報と、あるライフラインサービスの種類が決まれば、そのライフラインサービスが管轄する接続先が確定する。そこで、ENUMの枠組みにおいて、電話番号の代わりに、地理的位置情報とライフラインサービスの種類をキーとして用いれば、ENUMの枠組みをそのまま利用して接続先解決をすることができる。

このときに必要となる地理的位置情報の入手方法については次節で述べる。また、ENUMの枠組みにおいて地理的位置情報をキーとするには、電話番号のように扱いやすいことが重要であり、既存のエリアコードとして最も適切なものは、適度な粒度と階層構造を備えた郵便番号などが考えられる。ライフラインサービスの種類の指定は、地理的位置情報ベースのENUMにおける管理ドメインの下にサブドメインを設けることで、各サービス毎に個別の管轄区域を扱うことができる。

図4.1の中央部に地理的位置情報ベースでのENUM方式（位置依存型ENUM）の概念図を示した。この例では、ライフラインサービスとして警察を指定し、地理的位置情報として郵便番号630-0101の場合を示している。ENUMにおける電話番号の変換のときと同様に、郵便番号を逆順にしてドットをはさみ、上位に警察の指定を意味するpoliceを加えて、1.0.1.0.0.3.6.police.emergency.demoを対応したドメイン名として生成している。元々のENUMでのe164.arpaに対応する上位ドメインは別途決める必要があり、ここでは仮に、実証実験のデモンストレーションで用いた仮想的なドメインであるemergency.demoとしている。この生成されたドメインのNAPTRレコードをDNSにて引くことで、元々のENUMと同様に接続先URIのリストが得られる。ここでは、図4.1の下部に示すように、接続先として三つのインターネットアドレス(URI)が得られており、SIPアドレス

を用いて VoIP による音声や、文字や映像によるリアルタイム通信を行なうことができる。さらに、メールアドレスを用いてメールによる緊急通報をしたり、ウェブアドレスを用いてホームページへのアクセスやウェブ上でのインタラクティブ型の緊急通報も利用することができる。

このように、地理的位置情報ベースの ENUM 方式により、ライフライン通信に対する接続先情報管理サーバを、DNS サーバを用いて構築運用することができる。つまり、新たなデータベースシステムを構築する必要はない。そして、ENUM の標準化で現在進められているプロトコルやデータ形式に準拠することができるとともに、運用管理におけるノウハウについても利用でき、DNS そのものであることから各ライフラインサービスごとに分散運用管理や負荷分散などが可能である。

2. 地理的位置情報証明書

ここでは、ライフライン通信における発信者の居場所である地理的位置情報の取扱い方法として、網が地理的位置情報を提供し、かつ、保証する、地理的位置情報証明書方式を提案する。

2.1 網からのおよその位置情報の提供と保証

前章で述べたように、発信者端末が入手した GPS 情報を通知しても、通知を受けた側ではその情報の正当性を確認することができないといった問題がある。また、GPS 情報は必ずしもあらゆる環境で入手利用することができるわけではないという問題がある。そこで、ここでは、インターネット上において、網からおよその地理的位置情報の提供と保証をする枠組みを提案する。

発信者がアクセスとして利用しているローカルネットワーク側から見ると、自分のネットワークに現在接続して利用している利用者それぞれについて、どの利用者がおよそどこにいるかといった、およどの地理的位置情報を把握することができる。例えば、有線 LAN であれば Ether などで構築している範囲内であるし、

無線 LAN であれば基地局を中心に電波が届く範囲内である [25]。ADSL・CATV・FTTH などの場合は回線敷設先の地理的位置情報が利用できる。さらに、VPN やモバイル IP を用いている場合でも、気付アドレスの属するネットワーク側から把握することができる。

このように、発信者が今ちょうどアクセスに用いているローカルネットワークは、ある時刻において、ある IP アドレスを持つ端末が、およそどの場所にいるという情報を、提供かつ保証することができる。それに基づいて、そのローカルネットワークを管轄とする地理的位置情報管理サーバが、時刻情報、IP アドレス、地理的位置情報の三つの組み合わせ情報に署名することで、地理的位置情報証明書を発行する。そして、この地理的位置情報証明書によって、GPS などに依存することなくインターネット上から地理的位置情報を入手できるとともに、他の者へ通知をした時にも、網側から保証された正当性のある地理的位置情報として利用されることができる。

2.2 地理的位置情報証明書の発行

図 4.2 に地理的位置情報証明書の発行についての概要を示す。地理的位置情報管理サーバは、IP アドレス空間を管轄するルート CA あるいは上位空間 CA によって、自分が管轄するネットワークの IP アドレス空間に対する管轄の正当性を得るため、IP アドレス空間を対象とする IP アドレス空間公開鍵証明書の発行を受けておく（図 4.2 の (1)）。この例では、2001:200:169::/48 の IP アドレス空間をこの地理的位置情報管理サーバは管轄しており、この 2001:200:169::/48 を対象とする IP アドレス空間公開鍵証明書の発行を受けてサーバを運用している。そして、この IP アドレス空間公開鍵証明書を用いてユーザ端末からのリクエストに基づき、地理的位置情報証明書を署名発行する（図 4.2 の 2）。この地理的位置情報証明書の中身は、時刻情報、IP アドレス情報、地理的位置情報からなり、この三つの情報の組み合わせに対して、地理的位置情報管理サーバが保証を与えている。すなわち、ある時点においてある IP アドレスを持つ端末がおよそどこそこの地理的位置に存在しているということを保証する。

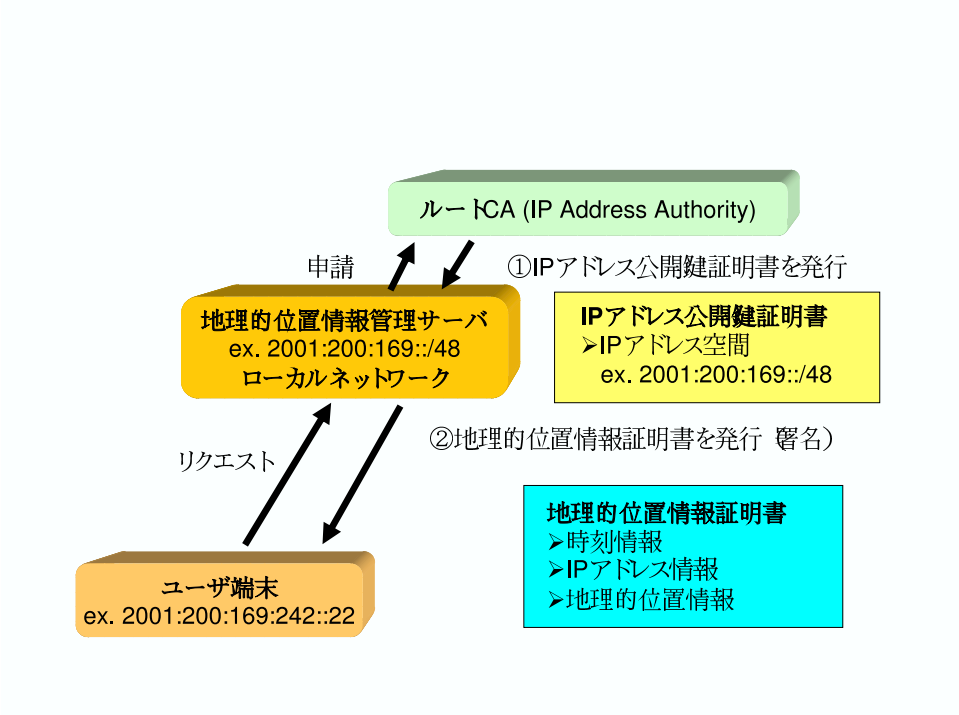

図 4.2 地理的位置情報証明書の発行

2.3 地理的位置情報証明書の通知と検証

図 4.3 に地理的位置情報証明書の通知と検証についての概要を示す。地理的位置情報証明書の発行を受けた発信者は、任意の通信相手へそれを送付することで通知することができる（図 4.3 の 1)。この地理的位置情報証明の通知は S/MIME 形式を用いて行なうことで、SIP （VoIP など通信）や SMTP (メール送信) や HTTP (ウェブアクセス) といった多くの通信プロトコルで親和性がよく、容易に扱うことができる。

接続先である通信相手（例えば、緊急通報の場合は警察や消防などのライフラインサービス機関など）においては、地理的位置情報証明書の通知を受けると、IP アドレス空間を管轄するルート CA からたどって、地理的位置情報証明書の署名者の正当性を検証できる（図 4.3 の (2))。これは、発信者が接続しているネットワーク側によって確かに証明書が発行されたことを確認するためである。さら

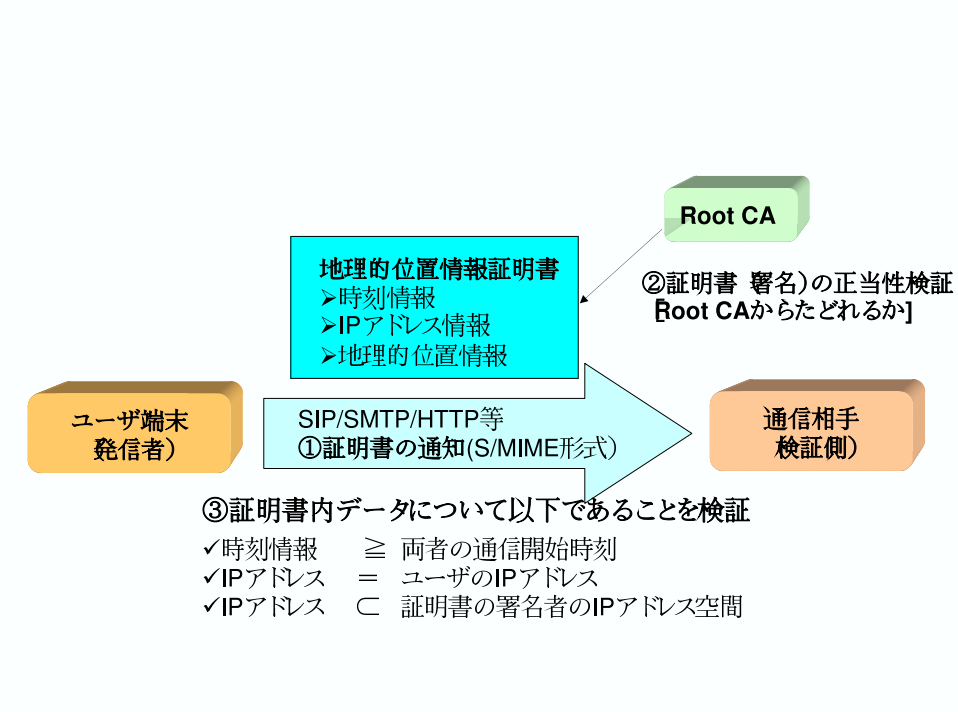

図 4.3　地理的位置情報証明書の検証

に、地理的位置情報証明書の中身のデータである時刻情報、IP アドレスを検証する（図 4.3 の (3)）。時刻情報を確認する理由は、証明書の再利用を防ぐためである。また、発信者が実際に用いている IP アドレスと、証明書内の IP アドレスが一致することも確認する。これは、確かにその発信者へ発行された証明書であることを確認するためである。さらに、その IP アドレスが、証明書の署名者の管轄 IP アドレス空間内であることを確認する。これは、管轄外の IP アドレスに対する証明書となっていないことを確認するためである。これらの確認によって証明書の正当性が検証されると、証明書内の地理的位置情報によって、発信者の現在のおよその居場所がどこであるかを、網側から確かに保証されたデータとして得ることができる。

2.4 地理的位置情報証明書とGPS情報

図4.4に地理的位置情報証明書とGPS情報についての特徴と関係を示す。発信者からは地理的位置情報証明書の通知に加え、発信者側で利用可能であればGPS情報の通知も受けることができる。このとき、GPS情報の方は証明書に比べて詳細な情報を示しているかもしれないが、GPS情報の通知単独では、発信者による詐称の可能性もある。一方、地理的位置情報証明書からの情報は、網側で把握できる範囲内のおよその地理的位置情報であるかもしれないが、発信者の意向とは独立に、網から提供された信頼性のある情報である。このように、両者の特徴はまったく逆であるとともに、互いに補完する関係にある。つまり、両者の情報を組み合わせることで、信頼性があり、かつ、詳細な地理的位置情報を得ることができる。

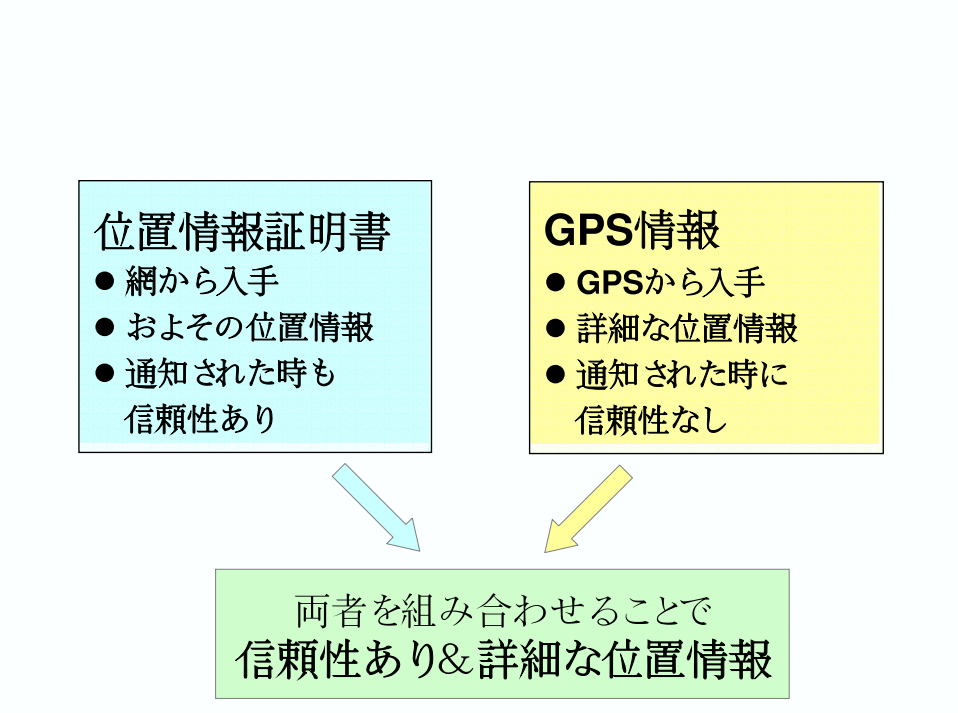

図 4.4 地理的位置情報証明書とGPS情報の関係

3. ユーザ情報証明書

ここでは、ユーザが属するホームドメインがユーザ情報を提供し、かつ、保証するユーザ情報証明書方式を提案する。ユーザ情報のうち最も重要なものは、インターネット上で用いられるユーザアドレスであり、一般的にユーザ@ドメインの形をとって、メールアドレスやSIP アドレスなどで用いられている。このユーザアドレスはライフライン通信で必要とされる呼び返しの実現においても必須となる。このユーザ@ドメインは、そのユーザがそのドメインに属していることを示しており、逆に言えば、ユーザを認証を行ないそのユーザアドレスの所有者であることを保証できる主体はそのドメイン、すなわちユーザにとってのホームドメインのみである。

このように、ユーザが所属しているホームドメインは発信者を認証することで、ある時刻において、あるIP アドレスを持つ端末が、自分のところに属するユーザであるという情報を、提供かつ保証することができる。それに基づいて、そのホームドメインを管轄とするユーザ情報管理サーバが、時刻情報、IP アドレス、ユーザ情報の三つの組み合わせ情報に署名することで、ユーザ情報証明書を発行する。

3.1 ユーザ情報証明書の発行

図 4.5 にユーザ情報証明書の発行の概要を示す。ユーザ情報管理サーバは、ドメイン名を管轄するルートCA あるいは上位空間のCA から、自分が管轄するドメイン名に対する管轄の正当性を得るため、ドメイン名を対象とするドメイン名公開鍵証明書の発行を受けておく（図 4.5 の (1)）。この例では、ユーザ情報管理サーバはドメイン名 test.demo を管轄しており、それに対するドメイン名公開鍵証明書を得ている。それを用いてユーザからのリクエストに基づき、ユーザ情報証明書をユーザへ署名発行する（図 4.5 の (2)）。このとき、地理的位置情報証明書の発行のときとは異なり、サーバはユーザが自分のドメインに属しているユーザであるかどうかを認証してから発行しなければならない。この例では、このドメインに属する user1 に対して認証した上で、このユーザが user1@test.demo で

あることを証明するユーザ情報証明書を発行している。

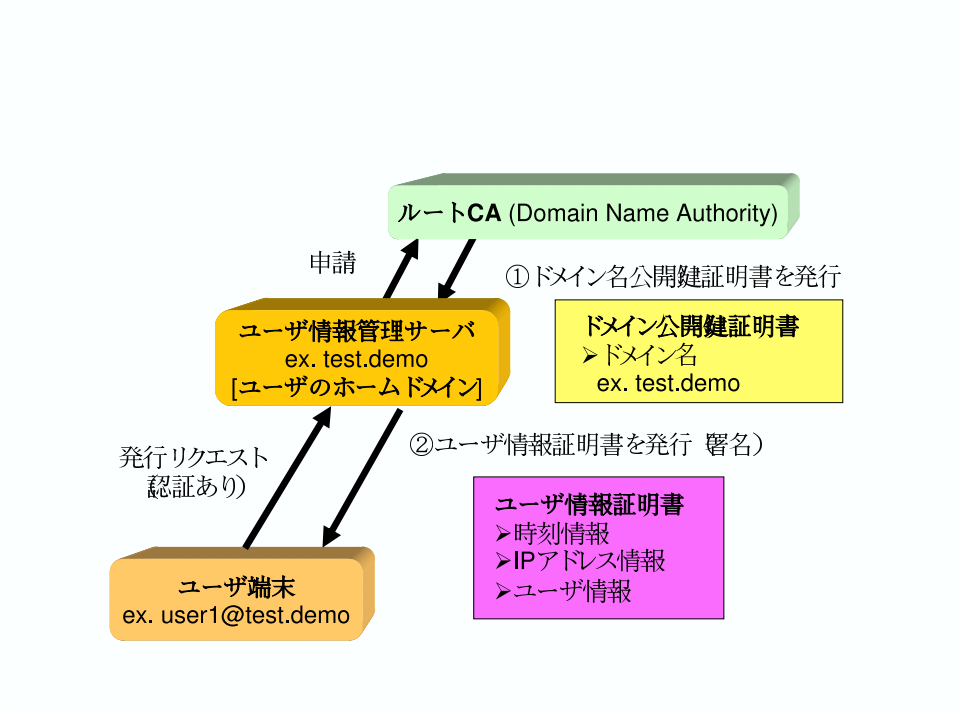

図 4.5 ユーザ情報証明書の発行

3.2 ユーザ情報証明書の通知と検証

図 4.6 にユーザ情報証明書の通知と検証についての概要を示す。ユーザ情報証明書の発行を受けた発信者は、任意の通信相手へとそれを送付通知することができる（図 4.6 の (1)）。通知の形式は地理的位置情報証明書と同様に S/MIME 形式をとる。したがって、VoIP などにおける SIP や、メールにおける SMTP や、ウェブアクセスにおける HTTP など、多くの通信プロトコルにおいて親和性があり通知することができる。警察や消防などのユーザ情報証明書の通知を受けた側では、ドメイン名を管轄するルート CA からたどって証明書の署名者の正当性を検証できる（図 4.6 の (2)）。これは、ユーザ情報証明書の発行が正規のもので

あることを確認するためである。さらに、証明書の中身である時刻情報、IP アドレス、ユーザ情報を検証する（図 4.6 の (3)）。時刻情報を確認するのは証明書の再利用を防ぐためである。また、発信者の用いている IP アドレスと証明書内の IP アドレスが同一であることを確認する。これは、この証明書が確かに現在通信中の発信者に対して発行されているものであることを確認するためである。さらに、発信者が用いているユーザアドレスと証明書内のユーザアドレスが同一であることを確認する。最後に、そのユーザアドレスが、証明書の署名者、すなわち、ユーザ情報証明書の発行者のドメイン内であることを確認することで、確かにそのユーザアドレスが所属するドメインにおいて発行されたものであることを検証する。これらの検証をすべて行なうことで、発信者のユーザ情報の正当性を確認することができる。

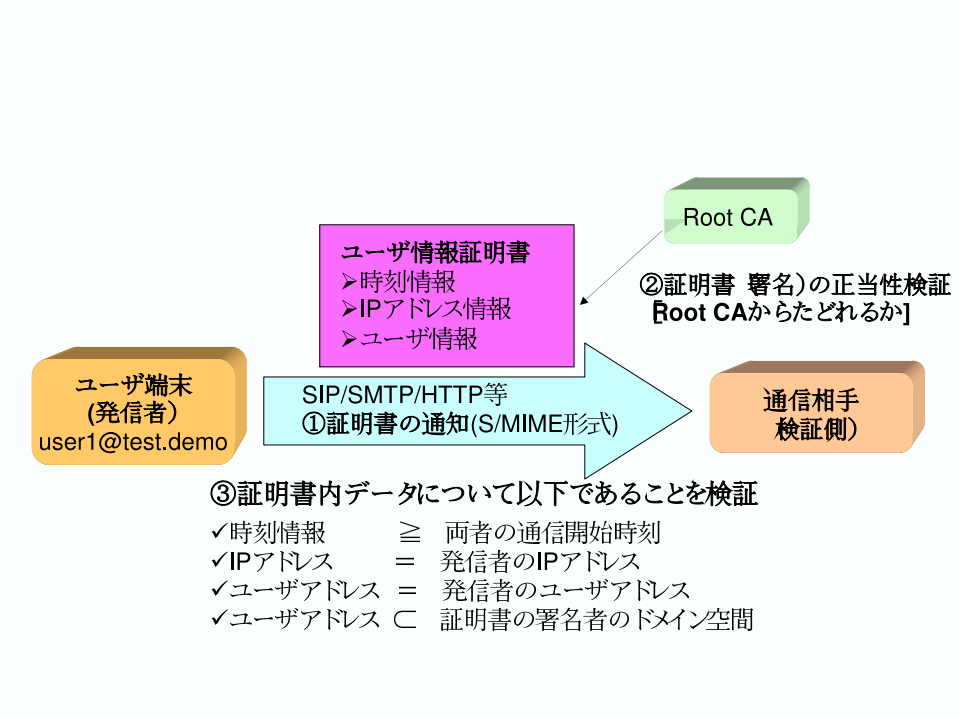

図 4.6 ユーザ情報証明書の検証

第5章　ライフライン通信システム

この章では、前章において提案した三つの方式、地理的位置情報ベースの ENUM 方式、地理的位置情報証明書方式、ユーザ情報証明書方式、に基づき構築した、インターネットにおけるライフライン通信システムについて述べる。

1. システム構成

ライフライン通信システム（図 5.1）の基本型は、ライフライン通信を行うユーザの発信側端末と、その発信側端末が接続しているローカルネットワークを管轄とする地理的位置情報管理サーバと、そのユーザの属しているホームドメインを管轄とするユーザ情報管理サーバと、地理的位置情報ベースの ENUM 方式（位置依存型 ENUM）による接続先情報管理サーバと、ライフライン通信の接続先であるライフラインサービス機関の端末から構成される。

この図 5.1 では、ライフライン通信のうち特に緊急通報型 (図 2.1) の構成を代表例としており、通信接続先の相手を警察・消防として図示している。例えば、安否登録・検索型 (図 2.3) の場合は、発信ユーザは被災者となり、その通信接続相手は安否情報登録データベースシステム等になる。また、安否連絡型 (図 2.2) の場合は、地理的位置情報に依存して接続先解決を行なう接続先情報管理サーバは用いられないが、通信接続相手が特定者となるだけで、他は同様の構成となる。情報取得・提供型 (図 2.4) の場合は、ユーザ情報証明書の利用がない形となる。

ここでは、すべての機能を含む緊急通報型を代表例として、以下にライフライン通信システムの構成の概要を説明をする。

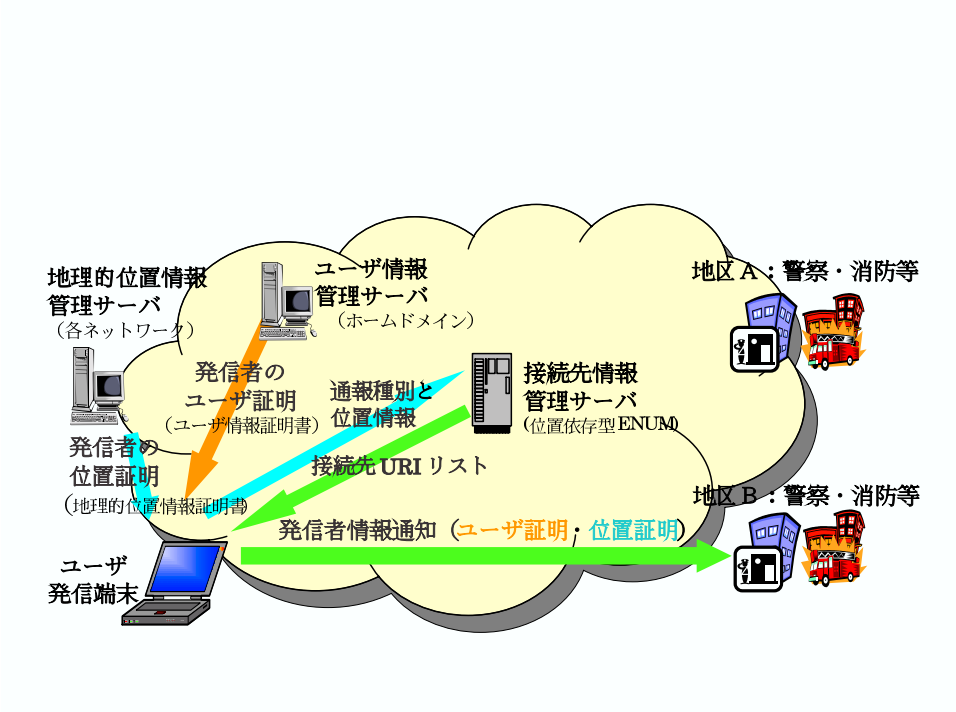

図 5.1　ライフライン通信システム

1.1　接続先情報管理サーバ

接続先情報管理サーバは、地理的位置情報ベースの ENUM 方式により接続先情報を提供し、元々の ENUM と同様に、実体は DNS サーバである。通常の DNS サーバと同様に階層構造に従って複数のサーバに分散して配置して運用することも可能である。

1.2　地理的位置情報管理サーバ

地理的位置情報管理サーバは、そのサーバが管轄する IP アドレス空間毎に、配置される。提供するおよその地理的位置情報のデータベースさえ共有していれば、複数の地理的位置情報管理サーバを配置して運用することも可能である。

1.3 ユーザ情報管理サーバ

ユーザ情報管理サーバは、そのサーバが管轄するドメイン名毎に、配置される。SIP による呼び返しを保証するため、SIP 登録サーバをユーザ情報管理サーバの一部として構成している。ユーザ情報管理のデータベースさえ共有していれば、複数のユーザ情報管理サーバを配置して運用することも可能である。

1.4 地理的位置情報証明書の入手

ユーザは好きなタイミングでいつでも、自分が利用しているネットワークの地理的位置情報管理サーバに対して、リクエストを発行して、地理的位置情報証明書を得ることができる。もちろん、GPS 装置を持っていれば、いつでも GPS による地理的位置情報も得ることができる。それらを定期的に行うことで、常に最新の地理的位置情報を保持することが可能である。

1.5 ユーザ情報証明書の入手

ユーザは好きなタイミングでいつでも、自分が属するドメイン名のユーザ情報管理サーバに対して、リクエストを発行して、認証を受けて、ユーザ情報証明書を得ることができる。ただし、その前に、ユーザ情報管理サーバの中の SIP 登録サーバに対して、認証を受けて、自分の IP アドレスを登録する必要がある。登録の有効期間が切れたときや、IP アドレスが変わったときにも、自分の IP アドレスを登録し直す必要がある。

1.6 接続先解決と証明書通知

ユーザがライフライン通信を開始するときは、入手している自分の地理的位置情報を利用して、接続先情報管理サーバから目当ての通信接続先（緊急通報の場合はライフラインサービス機関）の URI のリストを得る。そのあとは、元々の ENUM 使用時と全く同様に、通信手段を選んで、それに対応する URI を用いて通

信することができる。そして、ユーザは最新の地理的位置情報証明書とユーザ情報証明書を入手して、それらを通信相手へと送信する。それらの証明書はS/MIME形式を採用しているため、SIPやメールやウェブなどに親和性がよく、送信することができる。

1.7 各証明書の検証

通信相手は、前節までに定義した方式のモデルに基づいて、それぞれの証明書の正当性を検証する。そして、発信者のユーザアドレスと地理的位置情報を入手できる。もしそれらを入手できなかったとき、通信相手は、発信者からの通信を拒否することもできる。

2. ライフライン通信の流れ

ここでは、以上の提案した方法を用いたライフライン通信システムにおいて、実際にライフライン通信がどのように行なわれるかの一例を説明する。

図5.2は本研究において開発したシステムにおける、発信側の端末画面を表示している。発信側および着信側ともに、本研究において開発したアプリケーションを用いており、GUI操作と表示ができるとともに、ソフトフォン機能と文字会話機能を備えている。端末画面の中の各行は端末がやりとりしているプロトコルの概要を示しており、Sendは自分からの送信を、Recvは自分への受信を示している。これらのプロトコルのやりとりの表示により、動作の流れと情報のやり取りが目で見てわかるようになっている。

2.1 発信側端末の起動

発信側端末は、起動あるいはネットワークを移動したときなどにおいて、今回のシステムにおいては、IPアドレスの取得、SIPにおける登録動作、ならびに、地理的位置情報の取得を行なう。


user1@test.demo
Invite
OK
Cancel
Bye
Exit
Emergency Call
Police
Ambulance
Gas
Electricity
(01) Send SIP REGISTER sip:usr1@test.demo to 2001:200:169:24
(02) Recv SIP 401 Unauthorized [REGISTER] from 2001:200:169:
(03) Send SIP REGISTER sip:usr1@test.demo with Auth to 2001:
(04) Recv SIP 200 OK [REGISTER] from 2001:200:169:242::22
(05) Send HTTP GET /LocCertRequest [GeoLoc-Certificate] to 2
(06) Recv HTTP 200 OK [GeoLoc-Certificate] from 2001:200:169
(07) Initializaion OK
(08) Emergency Call Request Start
(09) Send NAPTR 1.0.1.0.0.3.6.police.emergency.demo [GeoENUM
(10) Recv NAPTR sip:request@nara-police.demo
(11) Recv NAPTR mailto:request@nara-police.demo
(12) Recv NAPTR http://www.nara-police.demo/
(13) Send SIP INVITE sip:request@nara-police.demo to 2001:20
(14) Recv SIP 100 Trying from 2001:200:169:252::7
(15) Recv SIP 180 Ringing from 2001:200:169:252::7
(16) Send HTTP GET /GPSData [GPS-Data] to localhost
(17) Recv HTTP 200 OK [GPS-Data] from localhost
(18) Send HTTP GET /LocCertRequest [GeoLoc-Certificate] to 2
(19) Recv HTTP 200 OK [GeoLoc-Certificate] from 2001:200:169
(20) Send HTTP GET /UsrCertRequest [User-Certificate] to 200
(21) Recv HTTP 401 Unauthorized [User-Certificate] from 2001
(22) Send HTTP GET /UsrCertRequest [User-Certificate] to 200
(23) Recv HTTP 200 OK [User-Certificate] from 2001:200:169:2
(24) Send SIP INFO [GPS-Data] to 2001:200:169:252::7
(25) Recv SIP 200 OK [INFO GPS-Data] from 2001:200:169:252::
(26) Send SIP INFO [GeoLoc-Certificate] to 2001:200:169:252:
(27) Recv SIP 200 OK [INFO GeoLoc-Certificate] from 2001:200
(28) Send SIP INFO [User-Certificate] to 2001:200:169:252::7
(29) Recv SIP 200 OK [INFO User-Certificate] from 2001:200:1
(30) Emergency Call Request End
(31) Recv SIP 200 OK [INVITE] from 2001:200:169:252::7
(32) Send SIP ACK sip:request@nara-police.demo to 2001:200:1
(33) Emergency Call Established
(34) Recv SIP BYE sip:usr1@test.demo from 2001:200:169:252::
(35) Send SIP 200 OK [BYE] to 2001:200:169:252::7
(36) Emergency Call Terminated

図 5.2 発信側端末画面

2.1.1 IP アドレスの取得

発信側端末の起動または移動において、最初にIPアドレスを取得することになるが、これはライフライン通信とは無関係に、インターネットを利用するために必要である。今回の例では、DHCPによって、IPアドレスの取得 (2001:200:169:242::20) と、DNSサーバのIPアドレスの取得が完了している。

2.1.2 SIP における登録

SIPを利用するユーザ端末は起動あるいは移動した際に、自分のホームドメインのSIP登録サーバへと認証登録を行なう。これはSIPにおける標準的な動作であり、ここでは自分が現在用いているIPアドレスで構成されたSIPアドレスである sip:usr1@2001:200:169:242::20 をコンタクトアドレスとして、自分の固有のSIPアドレスである sip:usr1@test.demo の登録更新を行なっている。これによって、自分の端末が移動してIPアドレスが変化した場合でも、それに関わらず一定した自分固有のSIP:ユーザ@ドメインのアドレスで呼び出しを受けることが可能となる。

図5.2において、プロトコル表示の行01から行04がこのSIPによる登録（REGISTER）プロトコルを示している。なお、このSIPの登録プロトコルではチャレンジ - レスポンス方式を利用したダイジェスト認証が行なわれているため、最初の行01の登録送信に対して、行02の受信においては一旦、認証エラー（Unauthorized）となり、再び行03にて認証付で登録送信を行ない、行04においてコンタクトアドレスの登録が成功となっている。この一連の部分は、SIPにおける標準的なプロトコルのやり取りである。この認証は、自分のホームドメイン（この例では test.demo ドメイン）での認証であり、そのユーザとそのホームドメインとの間で事前にパスワード付与などによって利用可能となっているものである。

2.1.3 地理的位置情報の取得

発信側端末は起動した時、あるいは、新たなネットワークに移動して接続した時などに、自分の新たな地理的位置情報をインターネットから入手する。これは、

自分がインターネットへのアクセスに用いているローカルネットワークを管轄とする地理的位置情報管理サーバから、地理的位置情報証明書の発行を受けることで、そのローカルネットワークが把握しているおよその地理的位置情報を入手する。もしも発信側端末が移動体であれば、定期的に、あるいは、随時必要な時に、新たな地理的位置情報を入手することができる。

図 5.2 において、プロトコル表示の行 05 が地理的位置情報証明書の発行リクエストであり、行 06 で地理的位置情報証明書を入手している。地理的位置情報証明書自体は S/MIME 形式となっており、地理的位置情報管理サーバからの入手においては HTTP の GET メソッドを用いた簡単な通信プロトコルで実装している。

この地理的位置情報証明書の取得においては、自分が用いている IP アドレスへの発行となるため、認証を必要としない。つまり、ユーザは移動先の接続ネットワークにおいても、そのネットワークへの接続自体の認証の有無とは無関係に、ネットワーク接続後は自分の地理的位置情報を入手することができる。

以上の SIP 登録と地理的位置情報の入手により、端末の起動時（あるいは移動時）の初期化が完了する（図 5.2 の行 07）。

2.2 ライフライン通信の接続先解決

2.2.1 ユーザからのライフライン通信呼び出し

今回の例のライフライン通信は、指定した相手への安否連絡などではなく、緊急通報呼び出しとなっている。そのため、このライフライン通信をユーザが行なう場合は、警察や消防といったライフラインサービスの種類を指定するだけで適切なその地域管轄のライフラインサービス機関を呼び出すことができる。なお、指定した相手への安否連絡など通信相手のインターネットアドレスが自明である場合は、ここからの接続先解決の部分を飛ばして、第 2.3.1 節のライフライン通信リクエストへと進む。

このライフラインサービス指定方法は、従来からの電話のように 110 番や 119 番のダイヤルによる指定、端末画面上のボタンを押したりメニューを選ぶことによる指定、あるいは、登録しておいた音声指示による指定など、様々なインタ

フェースが考えられるが、なんらかのユーザインターフェースによって、ユーザから端末へサービスの指定ができればよい。

今回の実装においては、端末画面上のボタンを押して指定する方法をとっている。図 5.2 の発信側端末の画面においては、上部の Emergency Call の選択行において、Police（警察)、Ambulance（消防）、Gas（ガス）、Electricity（電気）といったライフラインサービス指定のボタンを備えている。

今回のライフライン通信の例では、このうちの Police ボタンを押すことで、ライフラインサービスとして警察を指定している。これにより、発信側端末での緊急通報呼び出しが開始される（図 5.2 の行 08)。

2.2.2 接続先情報リストの取得

ユーザからのライフラインサービス種別の指定を受けた発信側端末は、その指定されたサービス種別と、入手してある地理的位置情報を用いて、地理的位置情報ベースの ENUM 方式（位置依存型 ENUM）により、接続先情報管理サーバ、すなわち、実体的には指定されたライフラインサービス種別の接続先情報を管理する DNS サーバより、接続先候補のインターネットアドレスのリストを取得することができる。

今回の例では、第 4 章第 1 節の地理的位置情報ベースの ENUM 方式の説明のところで示した図 4.1 と同様に、地理理的位置情報の指定に郵便番号〒 630-0101 を用いており、これは地理的位置情報証明書としてローカルネットを管轄する位置情報管理サーバから取得したものである。この地理的位置情報の指定、および、ここではライフラインサービスとして警察を指定することで、それらにより生成した 1.0.1.0.0.3.6.police.emergency.demo ドメインの NAPTR レコードを接続先情報管理サーバ（実体は ENUM と同様に DNS サーバ）へと問い合わせしているのが図 5.2 のプロトコル表示行 09 である。この問い合わせに対して、行 10 から行 12 が得られた NAPTR レコードであり、この例では、行 10 が SIP アドレス sip:request@nara-police.demo 、行 11 がメールアドレス mailto:request@nara-police.demo 、行 12 がウェブアドレス http://www.nara-police.demo/ の三つのインターネットアドレスが、接続先情報の候補リストとして取得できている。

この例ではそれぞれ１つずつのみ登録されているが、災害時などに代替施設でバックアップできるように、NAPTR レコードのプレファレンスを下げて（数値的には大きくして）、複数箇所の登録運用を行なうことができる。

2.2.3 接続先情報リストからの選択

このように、接続先候補のインターネットアドレスのリストが入手されたあとは、ユーザからの指定、あるいは、発信側端末の機能の制限によって、どの通信手段でライフライン通信を行なうかが決定される。例えば、メール送信しかできない端末であれば、ユーザからの指定なしにメールアドレスが自動的に選択される。

今回の実装例では、取得された接続先情報の候補リストの各行をユーザがクリック選択することで通信手段を選択する。今回の利用例では、SIP アドレス sip:request@nara-police.demo をユーザが選択し、SIP を用いたライフライン通信を行なう。

なお、今回の警察の例のようなライフラインサービス機関への通信ではなく、はじめから相手のインターネットアドレスがわかっている相手への安否通知といったライフライン通信を行なう場合は、これらの接続先情報の解決と接続先候補からの選択のフェーズは省略される。

2.3 ライフライン通信の接続と通知

2.3.1 SIP によるライフライン通信リクエスト

接続先と通信手段が確定すると、発信側端末は接続先との通信を開始する。図 5.2 におけるプロトコル表示の行 13 が SIP による通信の最初の INVITE リクエスト送信である。行 14 と行 15 において接続先である通信相手からの呼び出しを確認を受けている。これらはすべて通常の SIP による INVITE における通常の挙動である。

2.3.2 最新情報の取得

接続先へ最新の情報を通知するために、今回の例では、GPS 受信装置からの GPS 情報の取得と、地理的位置情報管理サーバからの地理的位置情報証明書の取得と、ユーザ情報管理サーバからのユーザ情報証明書の取得を行なう。

図 5.2 の行 16 と行 17 は、自分の発信側端末についている GPS 受信装置から GPS 情報の取得である。今回の実装においては、GPS 受信装置からの情報を端末内の GPS サーバによって管理しているため、GPS 情報の入手も地理的位置情報証明書の入手と同様に HTTP のプロトコルの GET メソッドにて行なっている。一般的に、GPS 受信装置は、もしあれば、自分の端末に備わっているものであるため、GPS 情報の取得自体は発信側端末のアプリケーションの実装に依存する。

行 18 と行 19 は地理的位置情報管理サーバからの地理的位置情報証明書の取得を行なっている。これは、第 2.1.3 節の地理的位置情報の取得と同じである。

行 20 から行 23 にかけては、ユーザ情報管理サーバからのユーザ情報証明書の取得を行なっている。ユーザ情報証明書は地理的位置情報証明書と同様に S/MIME 形式となっており、ユーザ情報管理サーバからの入手においては同様に、HTTP の GET メソッドを用いた簡単な通信プロトコルで実装している。また、このユーザ情報証明書の取得は、SIP による登録（REGISTER）と同様に自分のホームドメインに対して行なうため、全く同様にチャレンジ - レスポンス方式を利用したダイジェスト認証が行なわれる。したがって、行 21 の受信においては一旦、認証エラー（Unauthorized）となり、再び行 22 にて認証付で取得リクエストの送信を行ない、行 23 にてユーザ情報証明書の取得が成功する。

2.3.3 取得した最新情報の通知

次に、この例では、取得した最新情報である、GPS 情報と地理的位置情報証明書とユーザ情報証明書の通知送信を行なう。実際の運用においては、それぞれの情報の取得と通知を、すべて並行的に行なうことも可能であるが、今回の例ではわかりやすくするために、取得においても、通知においても、順次的に行なっている。

図 5.2 の行 24 から行 29 にかけてが、接続先への、GPS 情報と地理的位置情報証明書とユーザ情報証明書の通知送信である。これらの情報の SIP における送付方法としては、今回は INFO リクエスト [26] を用いており、そのボディ部に証明書を S/MIME 形式で格納している。SIP を用いたコミュニケーションいおいては、そのセッションが長時間確立したままで、その間に移動するなどして、最新情報を通知するという運用も考えられるが、INFO リクエストを用いているので情報の更新通知も可能となっている。

これらの情報通知を行なうことで、SIP におけるライフライン通信のリクエストが完了し、発信側端末においてはこのリクエストしたセッションの受理待ち状態となる（図 5.2 の行 30）。

2.4 ライフライン通信の受信と検証

2.4.1 発信者情報通知の受信

ライフライン通信のリクエストを受けた着信側端末の画面例を図 5.3 にて示す。この例では、緊急通報型となっていて、ライフラインサービス機関して仮想的な警察が着信側であり、発信側で指定した SIP アドレス sip:request@nara-police.demo を受理する着信側端末となっている。なお、緊急通報型以外においても、以下の説明は同様となる。

今回の実証実験例では、この SIP アドレス sip:request@nara-police.demo で呼び出されて着信できる端末は簡単に一つだけとなっているが、一般的な運用では、SIP が持つ標準的な機能にて、複数の端末へと着信を振り分けて、ライフライン通信リクエストを受信することができる。

図 5.3 の着信側端末において、行 03 から行 05 における SIP による INVITE リクエストと呼び出し確認は、図 5.2 の発信側端末における、行 13 から行 15 における SIP による INVITE リクエストと呼び出し確認と、送信（Send）と受信（Recv）がちょうど入れ替わって逆になっているだけで、全く同じものとなっている。また、図 5.3 の着信側端末においての、行 06 と行 07 における GPS 情報と、行 08 と行 10 における地理的位置情報証明書と、行 11 と行 13 におけるユーザ情報証明書

の通知についても、同様に、図 5.2 の発信側端末での行 24 から行 29 が対応している。

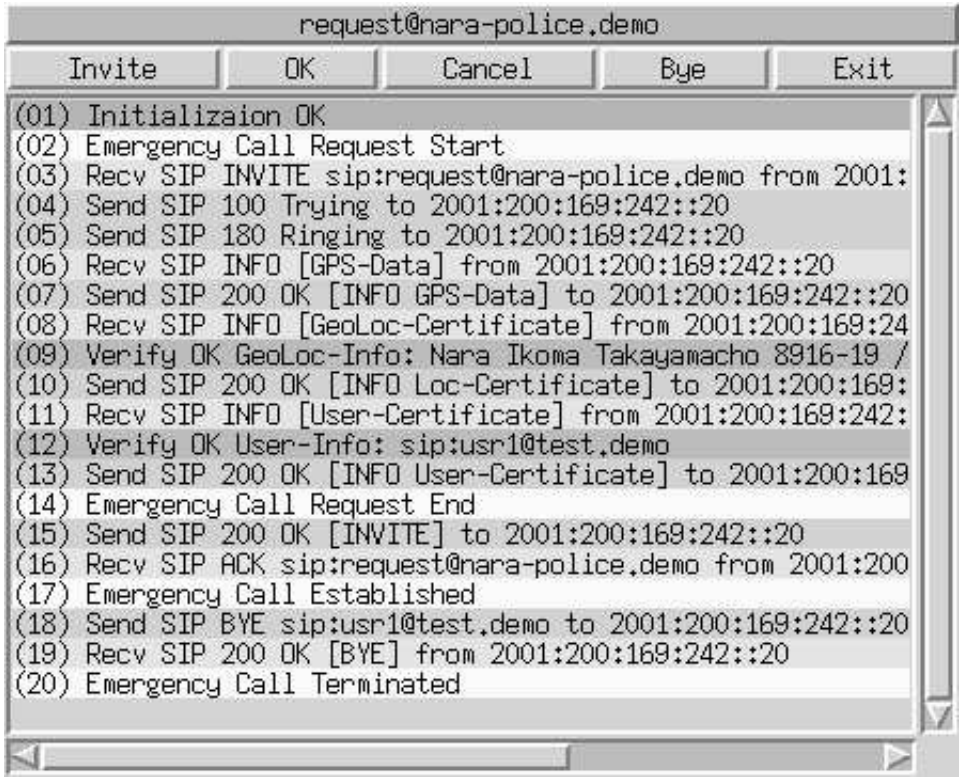

図 5.3 着信側の端末画面

2.4.2 地理的位置情報証明書の検証

このようにして各情報の通知を受けた接続先（この例では緊急通報先のライフラインサービス機関）である着信側においては、各情報の通知を受けたあと、各証明書が正当であるかどうかの検証を行なう。

図 5.3 の行 09 の Verify OK の行は、行 08 で通知を受けた地理的位置情報証明書の検証結果が OK であったことを示している。これにより、行 10 において発信側端末へ OK を返している。検証結果は、この行 09 をクリックすることで見ることができ、これを、図 5.4 にて示す。ここには、地理的位置情報証明書で得ら

れたデータ内容と、GPS 情報で得られたデータ内容と、地理的位置情報証明書が正当であるかどうかの検証結果の三つが示されている。

```
Geographic Location Information Certificate Data
  SerialNo=1
  IPAddress=2001:200:169:242::20
  GeoLocation=34 43 47.730 N 135 44 03.440 E 120m
        Countrycode=JP
        ZIP=630-0101
        A1="Nara"
        A3="Ikoma"
        A4="Takayamacho"
        A6="8916-19"
        NAM="TAO Nara Research Center"
  Date=Mon, 29 Mar 2004 06:18:19 JST
GPS Data
  GeoLocation=34 43 47.735 N 135 44 03.442 E 125.5m
Verification -> OK
  Certification = OK
  Date          = OK
   (Time 1080508699 >= StartTime 1080508698)
  IPAddress     = OK
   (IP 2001:200:169:242::20 = SenderIP 2001:200:169:242::20)
  AddressSpace  = OK
   (IP 2001:200:169:242::20 < Signer 2001:200:169::/48)
```

図 5.4 地理的位置情報証明書の検証

この地理的位置情報証明書の検証は、第 4 章第 2.3 節で示した図 4.3 のアルゴリズムにて行なう。まず、通知を受けた地理的位置情報証明書に対し、地理的位置情報証明のための IP アドレス空間管理のルート CA からたどることで証明書の署名者、すなわち、この証明書を発行した地理的位置情報管理サーバの正当性を検証できる。これにより、地理的位置情報証明書が正規に発行されたものであると確認される。

なお、地理的位置情報証明書自体は使い捨て型であるため証明書失効リストは存在しないが、IP アドレス空間公開鍵証明書のほうは IP アドレス空間の割り当てを受けている間のみ有効とするため、root CA による証明書失効リストの発行と、この検証過程における検査が必要となる。

その次に、地理的位置情報証明書に書かれているデータに対して検証を行なう。

まず、時刻情報が、発信側との通信開始時刻よりも以降であることを確認する。次に、IP アドレス（図 5.5 における 2001:200:169:242:20）が、発信側の IP アドレスと一致することを確認する。そして、この IP アドレスが、地理的位置情報証明書の署名者、すなわち、この証明書を発行した地理的位置情報管理サーバが管轄する IP アドレス空間（図 5.5 における 2001:200:169::/48）の中に入っているかどうかを確認する。これらを確認した上で問題なければ、発信側の地理的位置情報を確かなものとして入手利用することができる。

なお、通知で受け取った GPS 情報については、その性質から発信側による自己申告されたデータに過ぎないものであるが、地理的位置情報証明書によって示されている保証されたおおよその地理的位置情報のデータと比較することで、全く異なる場所からの詐称などを防ぐことができる。

2.4.3 ユーザ情報証明書の検証

図 5.3 の行 12 の Verify OK の行は、行 11 で通知を受けたユーザ情報証明書の検証結果が OK であったことを示している。これにより、行 13 において発信側端末へ OK を返している。検証結果は、この行 12 をクリックすることで見ることができ、これを、図 5.5 にて示す。ここには、ユーザ情報証明書で得られたデータ内容と、ユーザ情報証明書が正当であるかどうかの検証結果の二つが示されている。

このユーザ情報証明書の検証は、第 4 章第 3.2 節で示した図 4.6 のアルゴリズムにて行なう。まず、通知を受けたユーザ情報証明書に対し、ユーザ情報証明のためのドメイン管理のルート CA からたどることで証明書の署名者、すなわち、この証明書を発行したユーザ情報管理サーバの正当性を検証できる。これにより、ユーザ情報証明書が正規に発行されたものであると確認される。

なお、ユーザ情報証明書自体は使い捨て型であるため証明書失効リストは存在しないが、ドメイン名公開鍵証明書のほうはドメイン名の割り当てを受けている間のみ有効とするため、root CA による証明書失効リストの発行と、この検証過程における検査が必要となる。

その次に、ユーザ情報証明書に書かれているデータに対して検証を行なう。ま

```
User Information Certificate Data
  SerialNo=1
  IPAddress=2001:200:169:242::20
  UserAddress=usr1@test.demo
  Date=Mon, 29 Mar 2004 06:18:19 JST
Verification -> OK
  Certification = OK
  Date          = OK
   (Time 1080508699 >= StartTime 1080508698)
  IPAddress     = OK
   (IP 2001:200:169:242::20 = SenderIP 2001:200:169:242::20)
  UserAddres    = OK
   (User usr1@test.demo = Sender usr1@test.demo)
  DomainSpace   = OK
   (User usr1@test.demo < Signer test.demo)
```

図 5.5 ユーザ情報証明書の検証

ず、時刻情報が、発信側との通信開始時刻よりも以降であることを確認する。次に、IP アドレス（図 5.5 における 2001:200:169:242:20）が、発信側の IP アドレスと一致することを確認する。また、ユーザアドレス（図 5.5 における usr1@test.demo）が、発信側のユーザアドレスと一致することを確認する。そして、このユーザアドレスが、ユーザ情報証明書の署名者、すなわち、この証明書を発行したユーザ情報管理サーバが管轄するドメイン名（図 5.5 における test.demo）の中に入っているかどうかを確認する。これらを確認した上で問題なければ、発信側のユーザ情報を確かなものとして入手利用することができる。

これら、両証明書の検証とその結果に対する実際の運用方法としては、着信側であるライフラインサービス機関側などの通信相手の方針に応じて様々な運用方法が考えられる。例えば、各情報の通知を待たず、ライフライン通信リクエストを受理して通信確立するといった方法や、検証結果に関わらず参考データとしてみて、通信確立するといった方法もありうる。今回の例のにおいては、もっとも厳しい運用方法として、発信側の地理的位置情報とユーザ情報が正しく通知されてきているのを確認をしてから初めて、ライフライン通信リクエストを受理するといった運用方法となっている。すなわち、検証の成功をもってはじめて、図 5.3 の行 15 のように、SIP の INVITE リクエストに対する OK を送信している。

2.5 ライフライン通信の確立

発信側から着信側へSIPのACKが送信されて（図5.3の行16)、ライフライン通信の接続確立が完了する。このSIPのACKによる接続確立はSIPの標準機能である。

この接続確立によって、あとは、SIP利用における通常のリアルタイムコミュニケーションなどが行なわれる。本システムにおいては音声による通話と文字による会話を実証実験デモンストレーションのために実装した。

2.6 ライフライン通信の切断

SIPによるライフライン通信の切断においては、通常と同じく、SIPにおけるプロトコル上はBYEによって行なわれる。ライフライン通信のうち、警察や消防などのライフラインサービス機関との通信である緊急通報型においては、既存の固定電話のシステムには回線保留という機能が存在する。例えば、この回線保留の機能の一部の実現方法として、発信側からのBYEを行なわないといった運用は可能であるが、あくまでも発信側端末の挙動に依存するものであり、他から強制的に制御することができるものではない。一方、回線保留の目的は発信側への呼び返しであるため、ユーザ情報証明書により得られたユーザアドレスに対して呼び返しをすることで、その代替とする運用をすることが可能である。

3. システムの運用

3.1 IPアドレス空間に対するルートCA

地理的位置情報証明書方式の頂点となる信頼点が、IPアドレス空間に対するルートCA (IP Address Authority) である。このルートCAと、地理的位置情報証明書を発行する地理的位置情報管理サーバと、地理的位置情報証明書を通知するライフライン通信の発信者と、地理的位置情報証明書を検証するライフライン通信の着信者の関係を図5.6に示す。図の矢印１から３は実際にそれぞれの発行

と通知の通信が行なわれ、４の検証は信頼点としてのルート CA の公開鍵証明書の参照を示す。

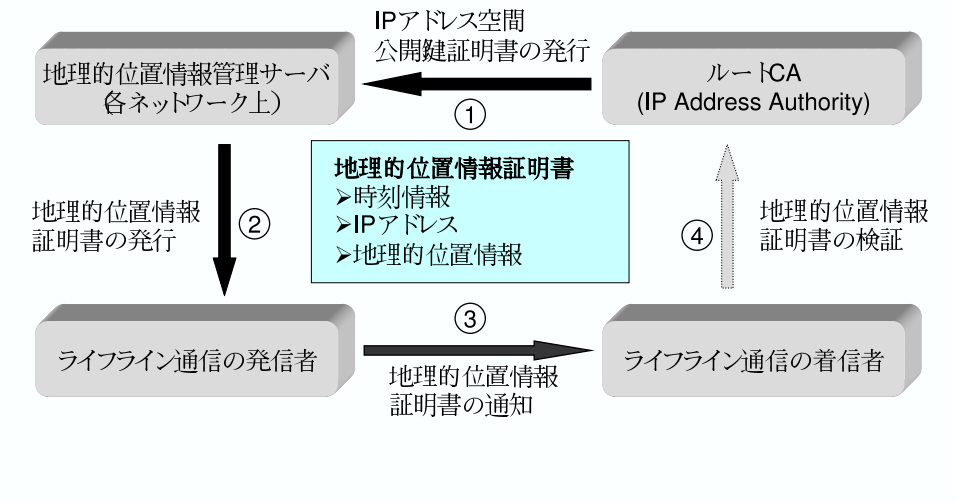

図 5.6 地理的位置情報証明書をとりまく関係図

このルート CA は、IP アドレス空間を割り当てられた組織への IP アドレス空間公開鍵証明書の発行とその無効の管理を行なう。特に、ここでの IP アドレス空間公開鍵証明書は、地理的位置情報証明書発行用のためのに発行される。

一方、地理的位置情報管理サーバは、IP アドレス空間を割り当てられた組織において運用され、その割り当てを受けた IP アドレス空間に対する IP アドレス空間公開鍵証明書をルート CA からあらかじめ発行しておいてもらい、それを利用して利用者からのリクエストに対して地理的位置情報証明書を発行する。

3.2 ドメイン名に対するルート CA

ユーザ情報証明書方式の頂点となる信頼点が、ドメイン名に対するルート CA (Domain Name Authority) である。このルート CA と、ユーザ情報証明書を発行するユーザ情報管理サーバと、ユーザ情報証明書を通知するライフライン通信の発信者と、ユーザ情報証明書を検証するライフライン通信の着信者の関係を図 5.7 に示す。図の矢印 1 から 3 は実際にそれぞれの発行と通知の通信が行なわれ、4 の検証は信頼点としてのルート CA の公開鍵証明書の参照を示す。

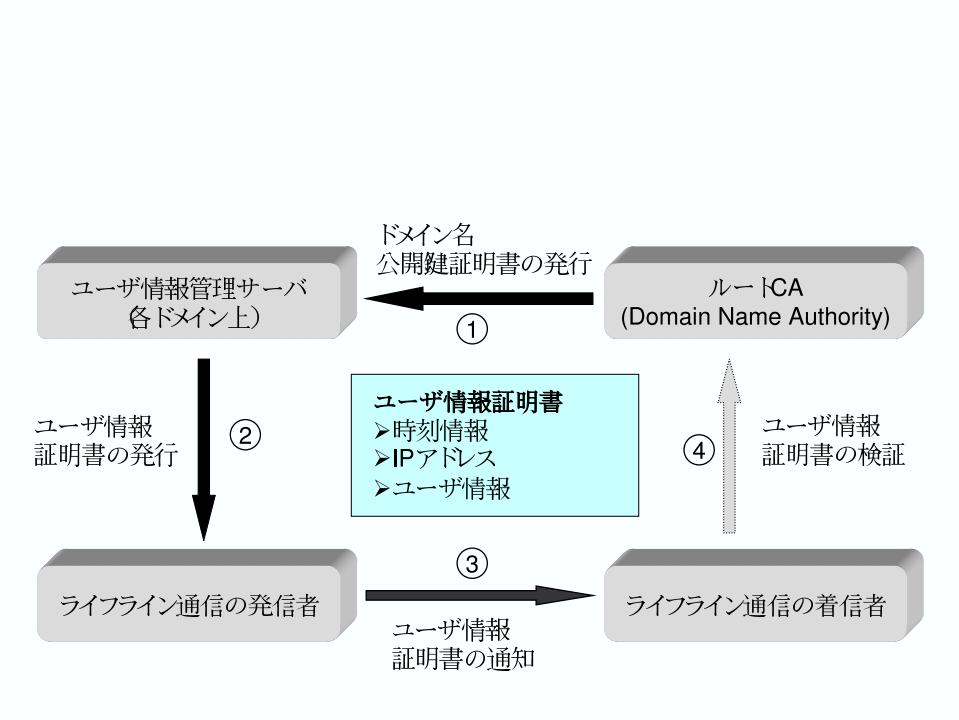

図 5.7 ユーザ情報証明書をとりまく関係図

このルート CA は、ドメイン名を割り当てられた組織へのドメイン名公開鍵証明書の発行とその無効の管理を行なう。特に、ここでのドメイン名公開鍵証明書は、ユーザ情報証明書発行用のためのに発行される。

一方、ユーザ情報管理サーバは、ドメイン名を割り当てられた組織において運用され、その割り当てを受けたドメイン名に対するドメイン名公開鍵証明書を

ルート CA からあらかじめ発行しておいてもらい、それを利用して利用者からのリクエストに対してユーザ情報証明書を発行する。

3.3 階層構造にそった中間 CA の配置

ルート CA と各組織のサーバとの間には、中間 CA を設置することができる。例えば、各 RIR (Regional Internet Registry) や各 NIR (National Internet Registry)、あるいは、各 ISP などにその中間 CA を設置することで、IP アドレス空間公開鍵証明書とドメイン名公開鍵証明書の発行において、それぞれルート CA への集中を避けることができる。

この場合、各中間 CA においては、IP アドレス空間あるいはドメイン名のサブセットとなる単位で管轄することになる。例えば、IP アドレス空間の場合、IP アドレス空間を管轄するルート CA から、2001:200::/32 を管轄する中間 CA がその IP アドレス空間公開鍵証明書の発行を受けることで、その IP アドレス空間の中のネットワーク 2001:200:169::/48 を持つ組織は、ルート CA からではなくその中間 CA から IP アドレス空間公開鍵証明書の発行を受けることになる。

また、各組織のネットワーク内における各サブネット毎の地理的位置情報管理サーバ配置の運用においても同様の方法をとることになる。例えば、ネットワーク 2001:200:169::/48 を持つ組織は、運用管理状況に応じて、そのサブネット 2001:200:169:100::/64 の IP アドレス空間公開鍵証明書を発行することで、そのサブネット上の地理的位置情報管理サーバを別個に動作させることが可能となる。このように IP アドレス空間の包含関係である階層構造を利用して、実運用における IP アドレス空間の委任や分割の状況をそのまま利用してスケーラブルな運用をすることができる。

同様にして、ドメイン名においてもその階層構造を利用してスケーラブルな運用をすることができる。例えば、ルート CA の下には国別インターネットレジストリである NIR が、各国の TLD (Top Level Domain) を管轄する中間 CA を設置することで、各国の TLD の下のドメイン名に対するドメイン名公開鍵証明書の発行を行なえる。同様に各組織のドメイン内では、サブドメイン名に対するドメイン名公開鍵証明書の発行をすることで、そのサブドメイン上のユーザ情報管理

サーバを別個に動作させることが可能となる。

3.4 各証明書の有効性と失効管理

ここでは、ライフライン通信システムで用いられる、地理的位置情報証明書、ユーザ情報証明書、IP アドレス空間公開鍵証明書、ドメイン名公開鍵証明書の四つの証明書それぞれについて、その有効性と失効管理について述べる。

3.4.1 地理的位置情報証明書

地理的位置情報証明書は、ある時点（あるいは保証可能な極短時間）でのみ有効な証明書であり、その時刻情報が証明書の基本要素の一つとなっている。つまり、その場かぎりでの使い捨て型であり、その時刻を過ぎたら無効となる。したがって、証明書失効リストの管理は不要である。

3.4.2 ユーザ情報証明書

ユーザ情報証明書も、ある時点（あるいは保証可能な極短時間）でのみ有効な証明書であり、その時刻情報が証明書の基本要素の一つとなっている。つまり、その場かぎりでの使い捨て型であり、その時刻を過ぎたら無効となる。したがって、証明書失効リストの管理は不要である。

3.4.3 IP アドレス空間公開鍵証明書

IP アドレス空間公開鍵証明書は、その組織に IP アドレス空間を割り当てている間のみ有効となるべき性質のものである。したがって、その有効期間はその割り当て期間と合致すべきであるが、一般には返却などによる IP アドレス空間の割り当て解除がいつになるかは予測できない。したがって、運用方法としては次の二つが考えられる。

一つは、証明書失効リストを用いて運用する方法である。発行する IP アドレス空間公開鍵証明書の有効期限は任意でよく、IP アドレス空間の返却などで無効

となれば、証明書失効リストによってその IP アドレス空間公開鍵証明書を失効させる。この方法での長所は、IP アドレス空間公開鍵証明書の発行とその更新を頻繁にしなくてよいように十分長い有効期限を設定できる点と、自由に IP アドレス空間の返却と、他者への再割り当てを行なえる点にある。一方、短所としては、証明書失効リストの管理が必要であり、これに伴い、地理的位置情報証明書の検証者においても、証明書失効リストの確認が必要となる。

もう一つ別の方法として、IP アドレス空間の再割り当てのための再利用に対し、再利用するまでの期間に制限を設けて運用する方法がある。すなわち、再利用禁止期間を設けるとともに、それと同じ有効期限にて IP アドレス空間公開鍵証明書を発行することで、もしも IP アドレス空間の返却がなされても、他者への再割り当てによる問題を防ぐことができる。この方法での長所は、証明書失効リストの管理が不要となることであり、これに伴い、地理的位置情報証明書の検証者においても、証明書失効リストのチェックが不要となる。一方、短所としては、IP アドレス空間の再割り当てに制限がかかって、ある一定期間は再利用できない点にあり、この期間を短くすると、IP アドレス空間公開鍵証明書の有効期限も短くなるため、頻繁にその更新発行をする必要となる。

3.4.4 ドメイン名公開鍵証明書

ドメイン名公開鍵証明書についても、IP アドレス空間公開鍵証明書の時と同じく、その組織にドメイン名を割り当てている間のみ有効となるべき性質のものである。同様に、証明書失効リストを用いる方法と、ドメイン名の再割り当て禁止期間を設ける方法の、二つの運用方法が考えられる。

3.4.5 証明書失効リストの確認

地理的位置情報証明書とユーザ情報証明書の検証者は、それぞれ、IP アドレス空間公開鍵証明書とドメイン名公開鍵証明書についての証明書失効リストの確認が必要となる。

もし、証明書失効リストの確認をしない場合、あるいは、できない場合は、な

りすましがあるかどうかを確認できない危険性があるが、失効したIPアドレス空間公開鍵証明書やドメイン名公開鍵証明書を用いることができるのは、以前に正当な割り当て対象者であった者である可能性が高く、リスクは限定される。

とはいえ、証明書失効リストの確認は必要であり、この確認によってライフライン通信の確立に遅延をおよぼす可能性もある。そこで、実際の運用方法としては、例えば緊急通報の際には、ライフライン通信の確立を先行させて、実際の緊急通報のやりとりと並行して、証明書失効リストの確認を行なうなどの運用上の工夫により、現実的な対応は可能となる。

3.5 接続先解決機構における運用

3.5.1 災害時等の迂回対策

ライフライン通信においては、災害などで支障が出た場合に代替施設へ迂回運用をする必要がある場合がある。例えば、既存の電話における緊急通報の場合、ある地区の通報受付施設が被災した場合などを考慮して、1時間以内を目標に接続先の切替を行なうことになっている。

本提案方式である、地理的位置情報ベースのENUM方式においては、DNSサーバである接続先情報管理サーバにおいてこれを対応することになり、これには二つの運用方法が考えられる。

一つは、接続先の切替が必要となる毎に、DNSの設定を書き換える方法である。この方法は柔軟な切替ができるという長所があるが、DNSの特性により、DNSキャッシュを考慮すると、実際に各ユーザが接続する先が切り替わるのが遅くなりうる欠点がある。また、柔軟な切替とはいえ、被災したことを把握してから切替対応を行なうことになるため、その対応までの間にどこにも接続できない空白の時間が生じる可能性もある。

もう一つは、あらかじめ複数の接続先候補を、preference値を変えて設定しておく方法である。この方法は、被災やなんらかの障害で第一候補の接続先と通信できなければ、そのままユーザ側が第二候補の接続先へ通信を試みることができるため、切替までの空白時間は生じない。また、DNSの設定はそのままであるた

め、DNS キャッシュのために切り替わるのが遅くなるという欠点も生じない。

表 5.1 接続先候補の設定例

```
NAPTR 100 10 "u" "E2U+sip" "!^.*$!sip:info@main.nara.police!" .
NAPTR 100 11 "u" "E2U+sip" "!^.*$!sip:info@[2001:200:169:100::10]!" .
NAPTR 100 20 "u" "E2U+sip" "!^.*$!sip:info@sub.nara.police!" .
NAPTR 100 21 "u" "E2U+sip" "!^.*$!sip:info@[2001:200:169:200::10]!" .
```

表 5.1 は、迂回先の接続先候補の設定例である。この例では、main.nara.police と sub.nara.police の二つの候補を設定しているが運用によっては複数設定可能である。

3.5.2 DNS 障害時への対策

表 5.1 は、迂回先の接続先候補の設定に加えて、DNS 障害等で最終的な IP アドレスが解決できないという障害の可能性も考慮して、IP アドレスによる URI 指定を含めた運用設定例となっている。

このような IP アドレスによる URI 指定は、ドメイン名による抽象化や、その接続先解決における複数候補指定などを用いることができない欠点を持っているが、DNS にてライフライン通信のための接続先情報分のゾーンのみをミラーしていれば、DNS 障害時にも接続が可能となる長所がある。なお、この IP アドレスによる SIP アドレス指定の場合でも、SIP の通常の proxy 機能によって、その指定された SIP サーバのレベルで最終的な通信を受ける複数の端末へと振り分けることができる。

4. システムの拡張

この節では、本論文で提案したライフライン通信システムに対する拡張について、検討する。

4.1 モバイル IP への対応

本システムは、利用者が自分の端末を持ち歩いて異なる場所にて用いることも対象としており、2 節で示したように、利用者が移動をして新たなネットワークに端末を接続した場合にも、動作可能である。すなわち、新たに接続したネットワークでの IP アドレスの後、それに対応する地理的位置情報証明書などを取得することができる。

一方、モバイル IP[27] を用いる場合、新たに接続した先のネットワークにおける IP アドレスである気付アドレスとは別に、自分のホームネットワークにおけるホームアドレスを使い続けることができるが、地理的位置情報証明書はあくまでも気付アドレスに対して発行されるため、そのままでは、ホームアドレスに対する位置情報証明をすることができない。

これに対応するには二つの方法が考えられる。一つは、気付アドレスとホームアドレスの対応付けを管理するホームネットワークが、気付アドレスに対する地理的位置情報証明書を利用して、ホームアドレスに対する地理的位置情報証明書を発行する方法である。これにより、そのホームアドレスと通信する相手は、同じ枠組みのまま地理的位置情報証明書を扱うことができる。

もう一つは、そのホームアドレスと通信する相手が、気付アドレスとホームアドレスの対応付けを把握管理している場合に、気付アドレスに対する地理的位置情報証明書を、そのままホームアドレスに対する地理的位置情報証明書として認識する方法である。

このようにして、ホームアドレスを用いた通信の場合でも、地理的位置情報証明書を扱えるように拡張することで、モバイル IP にも対応することができる。

4.2 地理的位置情報証明書の拡張

地理的位置情報証明書には、地理的位置情報管理サーバが把握している地理的位置情報が記載されており、その情報の精度は把握している範囲内で最も詳しい情報となる。ライフライン通信において地理的位置情報証明書を利用する多くの場合は、この把握している範囲内で最も詳しい情報が通信相手に伝われればよいが、

通信相手によっては、意図的に、精度の低い情報を伝えたい場合もありうる。例えば、ある相手に安否連絡をする際に、位置を詳細に特定するレベルの緯度・経度までは伝えたくない場合や、居場所に依存する情報取得をする際に、住所の詳細までは伝える必要がない場合などが挙げられる。

このような場合の地理的位置情報証明書の利用を考慮すると、ユーザによって精度が指定された地理的位置情報証明書が入手できることが望ましい。これは、発行を受けるユーザが地理的位置情報管理サーバに対して、記載して欲しい精度のレベルを指定し、サーバがそれに対応した地理的位置情報証明書を発行することで実現することができる。

第6章　システム評価

この章では、提案したライフライン通信システムについてのシステム評価を行なう。まず最初に、実装構築したライフライン通信システムについての性能面からの評価を行ない、次に、このシステムの性質面からの評価を行なう。最後に、他のシステムとの比較評価について論じる。

1. システム性能評価

通常のシステムに加え、このシステムは二つの新しい証明書を取り扱っている。そこでこの節では、まず、これらの証明書の仕様に関するシステム性能の評価として、証明書の鍵長を変化させることでの所要時間の測定評価と、証明書内のデータ長を変化させることでの所要時間の測定評価を行ない、証明書の取り扱いにおけるシステム性能の測定評価を行なう。最後に、ライフライン通信確立までの一連のプロトコルにおいて、それぞれの所要時間ならびに全体の所要時間を測定分析することで、評価を行なう。

1.1 証明書の鍵長に対する所要時間

このシステムにおいては、通常の SIP を用いた VoIP 通信などと比べて、証明書の発行と検証のオーバーヘッドが新たに付け加えられている。そこで、それらのオーバヘッドがライフライン通信に与える影響について調べる必要がある。そのため、証明書の取り扱いに関するオーバーヘッドの測定と、その結果の評価を行った。データ測定のためにシステムで用いた PC は Intel Pentium III 1200MHz である。

このシステムは、地理的位置情報証明書とユーザ情報証明書を発行するための署名のためにRSA/SHA1アルゴリズムを用いて実装されている。署名を発行するために必要とされる時間は、RSA秘密鍵の長さに依存して変化する。そこで、鍵の長さが変更されたときに、証明書の発行と検証のそれぞれについて、どのように所要時間が変化するかについての測定を行った。

表 6.1 鍵長に対する証明書取り扱いの所要時間

処理 ＼ 鍵長	512bit	1024bit	2048bit	4096bit
ユーザ情報証明書発行	2.71ms	13.79ms	82.20ms	555.46ms
地理的位置情報証明書発行	2.72ms	13.81ms	81.98ms	554.30ms
ユーザ情報証明書検証	1.38ms	2.53ms	6.38ms	19.81ms
地理的位置情報証明書検証	1.39ms	2.56ms	6.41ms	19.82ms

表6.1は、鍵の長さがそれぞれ512 bit、1024 bit、2048 bit、4096 bitの時の結果を示している。鍵の長さが大きくなるほど、所要時間は非常に大きくなる。しかし、検証における所要時間の増大は十分小さく、最大でも20ミリ秒程度である。現状十分な長さであるといわれて用いられている鍵の長さが2048 bitの場合、証明書発行時間は標準的なネットワーク遅延と比較して大きくないが、鍵の長さが4096 bitの場合は約0.5秒を要している。

1.2 証明書内のデータ長に対する所要時間

次に、証明書の中のデータの長さに応じて、証明書の取り扱いの所要時間がどのように変化するかについての測定を行った。実証実験で用いた地理的位置情報証明書におけるデータの長さは346 Bytesであり、ユーザ情報証明書については151 Bytesである。これらはとりあえず必要となる最小限のデータのみ含んでいるため、必要に応じて拡張してデータの長さが増大したときに、証明書の取り扱い所要時間がどのように変化するかを測定した。

表6.2は、データの長さがそれぞれ、現状のユーザ情報証明書で用いている151 Bytes、現状の地理的位置情報証明書で用いている346 Bytes、512 Bytes、1024

表 6.2 データ長に対する証明書取り扱いの所要時間

データ長 ＼ 処理	発行	検証
151Bytes (ユーザ情報証明書)	82.20ms	6.38ms
346Bytes (地理的位置情報証明書)	81.98ms	6.41ms
512Bytes	82.02ms	6.52ms
1024Bytes	86.36ms	6.43ms
1536Bytes	86.46ms	6.49ms
2048Bytes	86.51ms	6.59ms

Bytes、1536 Bytes、2048 Bytes の時の結果を示している。データの長さが大きく増えたとしても、証明書の発行や検証における取り扱い所要時間の変動はほとんどなく、証明書に含ませる情報を拡張してデータの長さが増えたとしてもほとんど影響がないと言える。

1.3 証明書の取り扱いにおけるシステム性能

ライフライン通信システムにおいて、導入された証明書の取り扱いをどれだけ捌くことができるかは、実用的であるかどうかという点で極めて重要である。図 6.1 は、証明書の発行と検証それぞれにおけるシステム処理性能を示している。システムにおけるライフライン通信受理機関側における証明書の検証の処理能力は、証明書の発行の処理能力に比べて高く、この測定を行なった Pentiumu III 1.2GHz の PC において、4096 bit 長の鍵を用いた場合でも、1 分間に約 3000 件 (すなわち 1 秒間に約 50 件) の処理性能を示している。

一方、ライフライン通信のうち緊急通報を例に現状を見てみると、110 番の通報件数は全国で年間約 1000 万件となっており、すなわち、全国で約 3 秒に 1 件となっている。通報発生の偏りを考慮しても、1 秒間に約 50 件より小さいと思われるが、現実には通報受付は各都道府県で分散して行なわれるとともに、それぞれにおいて複数台の証明書検証機器をいくらでも増やして対応することが可能なシステムであるため、実用面においてもシステム性能は十分であると言える。

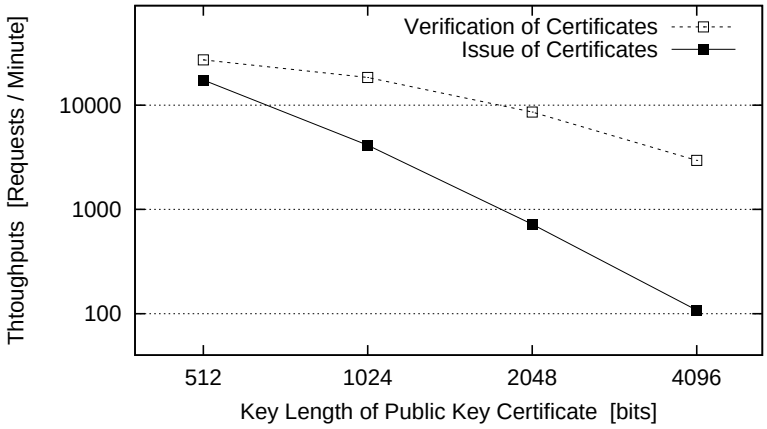

図 6.1 システム処理性能

1.4 ライフライン通信確立における所要時間分析

最後に、ライフライン通信を構成する各プロトコルにおける所要時間の解析を行った。これはそれぞれの項目でどの程度の所要時間がかかっているかを把握するためと、接続確立までにシステム全体でどれだけ所要時間がかかるかを把握するためである。

表 6.3 において、各行は、図 5.2 における各行と対応している。ネットワーク遅延による影響を避けるため、この性能測定実験は単一 LAN セグメント上において行った。また、表 6.1 の測定で用いられたのと同様に、鍵の長さをそれぞれ 512 bit、1024 bit、2048 bit、4096 bit とした時の所要時間を測定した。

表 6.3 が、得られた結果を示す。各時間は、前の行におけるイベントとその行におけるイベントの間で所要した時間を意味している。証明書の発行と検証における所要時間は、鍵の長さに応じて変化しており、それは、表 6.1 の測定結果と対応している。

表 6.3 は同一 LAN 上におけるライフライン通信の結果を示しており、WAN における実ネットワーク上での結果は、この LAN 上での測定時間に、各サーバとのネットワーク通信遅延、すなわち RTT (Round Trip Time) が付け加えられた合計時間になる。受信側が発信者情報をサーバに尋ねたりチェックしたりするシ

表 6.3 ラインライン通信における処理時間解析

(図 5.2 の番号) 処理	512bit	1024bit	2048bit	4096bit
(08) Request Start	-	-	-	-
(09) GeoENUM	0.1ms	0.2ms	0.2ms	0.2ms
(12) OK GeoENUM	5.8ms	5.9ms	6.0ms	5.9ms
(13) INVITE	13.9ms	14.2ms	13.8ms	13.8ms
(14) Trying	10.9ms	10.9ms	11.1ms	10.8ms
(15) Ringing	0.9ms	0.8ms	0.7ms	0.9ms
(16) GET GPS	1.9ms	1.6ms	1.7ms	1.8ms
(17) OK GPS	105.9ms	102.5ms	103.2ms	101.0ms
(18) GET GeoCert	0.7ms	0.7ms	0.7ms	0.7ms
(19) OK GeoCert	7.9ms	18.8ms	87.4ms	560.6ms
(20) GET UsrCert	0.5ms	0.5ms	0.5ms	0.5ms
(21) OK UsrCert	4.8ms	4.0ms	4.2ms	4.4ms
(22) GET UsrCert	0.7ms	0.7ms	0.8ms	0.7ms
(23) OK UsrCert	11.2ms	20.8ms	90.5ms	567.5ms
(24) INFO GPS	0.7ms	0.6ms	0.7ms	0.8ms
(25) OK GPS	8.2ms	8.1ms	8.7ms	8.5ms
(26) INFO GeoCert	0.6ms	0.6ms	0.7ms	1.1ms
(27) OK GeoCert	12.8ms	13.7ms	16.7ms	27.1ms
(28) INFO UsrCert	0.5ms	0.5ms	0.6ms	1.2ms
(29) OK UsrCert	13.2ms	13.6ms	16.1ms	25.5ms
(30) Request End	0.3ms	0.2ms	0.2ms	0.3ms
(31) OK INVITE	83.9ms	89.8ms	86.9ms	84.5ms
(32) ACK INVITE	0.9ms	0.9ms	0.9ms	0.9ms
(33) Established	0.3ms	0.4ms	0.3ms	0.3ms
Total Time	286.6ms	310.0ms	452.6ms	1419.0ms

ステムにおいても、同様にサーバとの間のこの RTT がかかる。

この測定実験の場合、発信者と受信者の間の通信において、三つの SIP INFO メッセージが順次的に往復している。しかし、これを並行的に送信するように最適化することは可能であり、その場合、余分にかかる遅延は発信者と受信者の間の往復時間一つ分のみとなる。

このようにして測定されたライフライン通信確立までの所要時間は、各証明書の発行と検証をそれぞれ含むため、鍵長 4096 bit の場合では約 1.4 秒となっている。

一方、これを現実の固定電話における通信確立までの所要時間と比較してみる。電気通信事業法の規定に基づいて定められた事業用電気通信設備規則においては、所要時間に関して二つの規定がある。一つは、事業用電気通信回線設備が発呼信号を受信した後、選択信号を受信可能となるまでの時間が 3 秒以上となる確率が 0.01 以下であることが求められている。しかし、これは、表 6.3 全体を意味する通信確立ではないため、本システムでは影響がなく特に問題はない。もう一つは、事業用電気通信回線設備が選択信号送出終了を検出した後、発信側の端末設備等に対して着信側の端末設備等を呼び出し中であること又は着信側の端末設備等が着信可能な状態でないことの通知までの時間が 30 秒以下であることが求められている。これは、本システムにおいて証明書の検証まで含めた全体の接続確立と解釈することもでき、その場合においても、本システムで新たに余分にかかる所要時間は比較して十分に小さいため、問題がないと言える。

2. システムの性質評価

ここでは、本システムの性質評価として、システムのスケーラビリティと頑健性、ならびに、セキュリティとプライバシーに関する考慮などについて論じる。

2.1 システムのスケーラビリティ

2.1.1 地理的位置情報管理サーバの配置

地理的位置情報管理サーバは、そのサーバが管理しているネットワーク上にいるユーザによってのみ利用される。すなわち、地理的位置情報証明書を発行する地理的位置情報管理サーバは、各運用管理ネットワーク毎に用意することできる。そして、そのサーバが管轄範囲とするネットワークに接続しているユーザだけが、そのサーバの利用者となって、地理的位置情報証明書の発行リクエストを出す。つまり、各管轄ネットワーク毎に分散して地理的位置情報管理サーバを配置でき、サーバが対応をすべきユーザも限定されていることから、スケーラブルな構成となっている。

さらに、このサーバは各組織のネットワークあるいは各サブネット毎に配置することが可能である。また、各管轄ネットワーク毎それぞれにおいても、地理的位置情報管理サーバを一つだけではなく、必要に応じて複数配置することで、複数のサーバを同じネットワーク上で機能させることもできる。このため、負荷分散や対障害性などのための多重化も可能となっており、地理的位置情報サーバの運用に関するスケーラビリティには問題がないと言える。

2.1.2 ユーザ情報管理サーバの配置

ユーザ情報管理サーバは、サーバが管理するドメインに属するユーザによってのみ利用される。すなわち、ユーザ情報証明書を発行するユーザ情報管理サーバは、各運用管理ドメイン毎に用意することできる。そして、そのサーバが管轄範囲とするドメインに所属しているユーザだけが、そのサーバの利用者となって、ユーザ情報証明書の発行リクエストを出す。つまり、各管轄ドメイン毎に分散してユーザ情報管理サーバを配置でき、サーバが対応をすべきユーザも限定されていることから、スケーラブルな構成となっている。

さらに、このサーバは各組織あるいは各サブドメイン毎に配置することが可能である。また、それらの各管轄ドメイン毎それぞれにおいても、ユーザ情報管理サーバを一つだけではなく、必要に応じて複数配置することで、複数のサーバが

登録データベースを共有しながら同じドメイン上にて機能することもできる。このため、負荷分散や対障害性などのための多重化も可能となっており、ユーザ情報管理サーバの運用に関するスケーラビリティには問題がないと言える。

2.2 セキュリティとプライバシー

地理的位置情報証明書とユーザ情報証明書は、他の者がそれらを入手して再利用することを防ぐため、時間情報を含んでいる。また、時間情報自体が証明される対象となっているため、これらの証明書は通信記録としてもしようすることができる。

プライバシーを守るため、これらの二つの証明書は分離して設計されており、利用者は必要に応じて片方の証明書のみを相手に送付することが可能である。そして、両方の証明書を受け取った者のみが、発信者が誰であり、かつ、どこにいるか、といった重要なプライバシー情報を知ることができる。

2.3 システムのリスクと頑健性

ここでは、このライフライン通信システムが正常に動作するためには、それぞれどの相手とどのような通信ができる必要であるかを述べるとともに、問題があった場合のリスク、ならびに、代替処置や対策について示すことで、システムの頑健性について論じる。

2.3.1 発信者側での要件

発信者においては、以下の各々と通信することができる必要がある。それらは、発信者のローカルネットワーク上にある位置情報管理サーバ、発信者のホームドメイン上にあるユーザ情報管理サーバ、接続先情報管理サーバ（位置依存型ENUM)、接続先の通信相手である。さらに、接続先情報管理サーバから得られるインターネットアドレス (URI) が対応する IP アドレスへと解決される必要がある。

2.3.2 接続先側での要件

発信者から通信を受けた接続先の通信相手側、例えば、緊急通報の例では呼び出しを受けたライフラインサービス機関などにおいては、発信者側から受理した地理的位置情報証明書やユーザ情報証明書を原則としてローカルに検証することができるので、基本的には他のサーバとの通信は発生しない。ただし、そこで用いられている IP アドレス空間公開鍵証明書やドメイン名公開鍵証明書に対する証明書失効リストの確認のための通信が発生する。

2.3.3 地理的位置情報管理サーバと通信できない場合

発信者が自分が現在使っているネットワークの地理的位置情報管理サーバを通信できない場合、地理的位置情報証明書を利用することができなくなる。すなわち、発信先において、発信者側から告知された地理的位置情報の正当性を確認することができず、その地理的位置情報はあくまでも発信者側から自己申告してきたものという位置付けになることを認識する必要がある。

一方、地理的位置情報管理サーバは自分が現在使っているネットワークにおいて配備運用されるため、発信先と通信できるにもかかわらず、複数の地理的位置情報管理サーバのいずれとも通信できないリスクは低い。

2.3.4 ユーザ情報管理サーバと通信できない場合

発信者が自分が属するホームドメインのユーザ情報管理サーバを通信できない場合、ユーザ情報証明書を利用することができなくなる。すなわち、発信先において、発信者側から告知されたユーザアドレスの正当性を確認することができず、そのユーザアドレスはあくまでも発信者側から自己申告してきたものという位置付けになることを認識する必要がある。

例えば、それをそのまま信じて発信者への呼び返しを行なうことはできない。しかし、このような異常事態においても、発信者の移動などで IP アドレスが変化しない限り、緊急時には、発信者が用いていた IP アドレスへの呼び返しを試みることは可能である。

2.3.5 接続先の名前解決ができない場合

発信者のローカルネットワーク上の DNS サーバが、接続先情報管理サーバからライフライン通信の接続先情報のゾーンのデータをミラーリングしていて、かつ、データ中のインターネットアドレスが IP アドレスベースである場合（例えば、sip:request@[2001:200:169::100] のような場合）、緊急通報時に接続先の IP アドレスを解決するために、接続先情報管理サーバや他の DNS サーバに依存しなくてすむため、それらへの IP 到達性は必要としなくなる。

2.3.6 最小限構成での動作

以上で述べてきた対策をとった場合、このライフライン通信システムは、ローカルネットワーク上のサーバと接続先（例えば緊急通報の場合はライフラインサービス機関）への IP 到達性のみに依存して、動作することができる。

2.4 本提案の証明書方式の評価

本提案方式においては、地理的位置情報証明書およびユーザ情報証明書ともに証明書方式をとっている。ここでは、証明書方式による一般的な利点と、本提案方式による付加的な利点それぞれについて述べる。

2.4.1 インターネット標準との親和性

本提案方式による証明書も、PKI [28] という標準的な枠組みの上に乗っており、各証明書の発行のための署名方式や、各証明書自体の検証方式についても標準的なライブラリなどで構成できる。また、各証明書の発行や通知の通信においては、S/MIME 形式 [29] を採用しており、これにより SMTP・HTTP・SIP など色々なプロトコルを用いて通知が標準的な方法で容易に可能となっている。

2.4.2 証明書の検証

証明書方式を用いることで、通信相手先では情報の正当性の検証を、他のサーバ問い合わせなどを行なうことなく、ローカルに行なうことができる。また、必要であれば通信途中のプロキシサーバなどにおいて情報を参照したり検証したりすることも可能である。

2.4.3 ユーザ端末における証明書の取り扱い

本提案方式の各証明書は、公開鍵証明書ではなく、必要な情報の組合わせをサーバ側で保証するために署名することで発行された証明書であるため、ユーザ端末側では各証明書を単なるデータの一種として特別な処理をすることなく、そのままの形にて転送することで相手先へ通知することができる。

2.4.4 再利用の防止

各証明書には発行されたときの時刻情報が含まれているため、自分あるいは他の誰かによって、後から別の時間に再利用することはできない。つまり、使い捨て型の証明書となっている。また、発行を受けた端末の IP アドレス情報が含まれているため、同じ時間に他の場所で発行を受けた証明書をなりすましなどのために転用することはできない。

2.4.5 通信記録としての証明書

各証明書には発行されたときの時刻情報が含まれているため、各証明書の通知を受けた側にとっては、時刻情報を含む通信記録の証明書として位置付けることも可能である。一方、証明書を用いずにサーバ問い合わせ方式だと、過去の状況についてもサーバへ問い合わせをしなければ正当性のある情報はわからないし、そのサーバ側で過去の履歴を保持する必要がある。本提案方式では、各証明書単体で正当性のある記録となりうる。

2.4.6 二つの証明書の分離

地理的位置情報証明書とユーザ情報証明書の両証明書は別々に用意されているため、用途に応じて、いずれか片方だけの発行を受けたり、いずれか片方だけを通知することが可能である。これによって、地理的位置情報証明書の通知を受けた者は、その端末がおよそどの位置にいるかといった情報だけ知ることになり、ユーザ情報証明書の通知を受けた者は、その端末を用いているのが誰であるかといった情報だけを知ることになる。これにより、どこにいるか、および、誰であるか、という二つの個人情報の管理を本人が別々に行なうことができ、プライバシー保護の要件を満たすことができている。そして、両方の証明書の通知を受けた者のみが、どこにいるか、および、誰であるか、の両方を知ることができ、それによって初めて、あるユーザがどこにいる、という合成した情報を入手することができる。

3. 他の方式との比較評価

ライフライン通信システムは、第3章で整理した要求条件を満たすように、第4章で提案した三つの方式によるモデルに基づいて構成されている。ここでは、それらの課題である、接続先解決方式、地理的位置情報の取扱い方式、ユーザ情報の取扱い方式のそれぞれについて、他の方式との比較評価することで、本論文で提案した方式の優位性を論じる。

3.1 接続先解決方式における比較評価

インターネット上における接続先解決の方式について、他の方式と本提案方式との比較評価についての説明を行なう。

3.1.1 IP ルーティング方式

接続先解決方法として、IP ルーティングの層で行なう方法が考えられる。そのうち一つとしては、ライフライン通信のような特番利用に対応する IP パケットになんらかの印を付け、各ルータで処理させる方式が考えられるが、ルータへの新たな機能拡張と負荷増大を伴うため困難であるとともに現実的ではない。

一方、現状のルータや運用管理でも適用できる方法として、IP エニーキャスト [30] 等により最寄りのホストへルーティングするといった方法が考えられる。IP エニーキャストは、例えばあるサービスを提供しているサーバのうち、ネットワークのトポロジ上の最寄りのサーバとの通信を実現するしくみである。

しかし、災害時等による障害を考えると、特定の接続トポロジーに依存した環境を想定した方式では非常に問題がある。また、一般に、インターネットを構成するトポロジは地理的な位置関係とは無関係に成り立っており、同じ県内のインターネットユーザが県外を通して通信することになるなど日常茶飯事となっている。この点を解決するには、地域 IX (Internet Exchange) を設けたり、すべての ISP や各接続組織などが個別に各ライフラインサービス機関などすべてと接続することにより、IP ルーティング技術を駆使することで、ある程度は解決することができる可能性がある。ところが、それでもなお、一般には地域 IX といってもせいぜい都道府県単位しか想定されておらず、消防・救急サービスのようにもっと細かい市町村単位などで接続先が変わる場合には対応できない。このように、インターネットの接続トポロジと各ライフラインサービスの個別管轄区域の違いを一致させることによって対応する方法は現実的ではなく困難である。

したがって、特番などをそのまま IP 層におけるルーティングによって解決する方式はできないため、事前に、対応する接続先のインターネットアドレス、あるいは、さらに IP アドレスを解決してから通信を行なう方法が望ましい。これはインターネットにおいては一般的な方法であり、例えば VoIP において一般の電話番号に電話する時に用いられる ENUM も、事前に電話番号に対応する接続先のインターネットアドレスを解決する方式である。また、電子メール配送においても、メールアドレスに対応する接続先のメールサーバを同様に DNS 上で解決してから配送通信を開始している。

3.1.2 DHCP サーバなどから情報提供する方法

地理的位置情報ベースの ENUM 方式を用いて接続先解決をせずに、最初から、接続先情報を DHCP や IPCP などで配布する方式が考えられる。また、地理的位置情報管理サーバから地理的位置情報証明書と同時に接続先情報を配るという方式が考えられる。それぞれ、地理的位置情報を提供できるのであれば、そこで、その地理的位置情報に対応する接続先情報も同時に提供できるというわけである。

しかし、接続先情報は地理的位置情報だけで確定するわけではなく、電気・ガス・水道・消防・警察といった多様なライフラインサービスの種類毎にそれぞれ異なるため、DHCP などで提供する時点ではこれが確定していないことから、すべてのサービスについての接続先情報を提供しなければいけないことになってしまう。さらに、各ライフラインサービスの種類毎の接続先情報についても、メールやウェブや SIP など多様な通信手段それぞれのインターネットアドレスが、バックアップを含めて優先順位情報などとともに複数含まれており、全体として非常に大きなデータとなってしまう。

また、DHCP サーバあるいは地理的位置情報管理サーバがこれらの情報をユーザ端末に提供するには、変更管理維持といった面から、自分のところでそれらの情報を静的に持つわけにはいかないため、結局は、どこかから情報を入手する必要がある。そのため、地理的位置情報ベースの ENUM 方式によって実現される接続先情報管理サーバ（実体は DNS サーバ）の存在自体は不可欠になる。そして、DHCP サーバなどは、単に接続先情報管理サーバから得た情報をリレーするだけの存在になってしまう。

一方、本提案方式の場合は、ユーザ端末が地理的位置情報ベースの ENUM 方式による接続先情報管理サーバから直接情報を得るので、利用するライフラインサービスの種類についての情報のみを入手することも可能であり、情報源から直接入手することができる。それに加え、情報入手のための通信プロトコルやその情報データ形式は元々の ENUM と全く同じであるため、新たな通信プロトコルやデータ形式を必要とせず、実装面でも運用面でもほぼ同じように利用することができる。したがって、ユーザ端末が直接、接続先情報管理サーバから情報入手するほうが好ましい。

3.1.3 集中受付ゲートウェイ方式

接続先解決をユーザやISP側などで一切行なわずに、各ライフラインサービス毎に集中受付ゲートウェイを設置する方法が考えられる。例えば、消防署の集中受付ゲートウェイを全国に１つ（あるいは複数）設置し、全国あちこちからのすべての緊急通報はそこへ接続させる方式である。この場合でも最終的には各市町村や地域の消防署へ通信なり転送なりする必要がある。いったん電話を受付けて居場所を尋ねてから各地へ回すといった事態を避けるには、通報者の地理的位置情報を利用して自動的に各地へ回すといったことが考えられる。

しかし、この方法では二つの問題が挙げられ、一つ目は集中型になっているために負荷分散が難しい点であり、もう一つは、経路上迂回するという点である。例えば、集中受付ゲートウェイを介さずに自分のいる地域の担当管轄の署へ直接通信すれば、もしもIPルーティング層レベルでその地域や地方の中で経路が閉じている場合、他地区の影響を受けないか最小限に抑えることが可能であるのに対し、集中受付ゲートウェイ方式では他地区へと経路上迂回してしまう可能性が高い。この問題を解決するために、もし、集中受付ゲートウェイを自分の地域に設置できて、自分の居場所に応じてそれを選択できるのであれば、最初からゲートウェイを介さなくてもよいことになる。また、ゲートウェイにて自動的に各地へ回すことができるのであれば、その情報を用いてユーザ側で最初から目的の地元の機関へと接続すればよいことになる。今回の提案方式では、これらの問題を回避し、あらかじめ接続先を解決してから接続のための通信を行なう方法をとっている。

3.1.4 ENUM以外の枠組み利用

このように、インターネット上におけるライフライン通信の接続先解決は、発信者側においてIP層ではなく上位層で行なう必要があるが、本提案方式で用いているENUMの枠組み以外の方法も考えられる。つまり、地理的位置情報とライフラインサービスの種類を指定したときに、それに対応する接続先のインターネットアドレスのリストを返す枠組みは、必ずしもENUMと同様の枠組みを用

いなくても実装することはできる。

しかし、本方式が使っているDNSを用いたENUMの枠組みはインターネット標準として整備されつつあり、運用管理の規定やノウハウといった面から実装や普及の面に至るまで、様々な点でENUMと同じ枠組みに準拠することの利点が大きい。地理的位置情報ベースのENUM方式を用いることは、元々ののENUMを実装している端末側にとっても利点がある。また、接続先情報管理サーバは、実際にはDNSサーバの一つとなることから、構築から管理に至るまで、サーバの運用側にとっても利点が大きい。さらに、DNS一般の利点である、サーバの分散化や多重化の恩恵も受けることができるとともに、DNSのセキュリティ拡張であるDNSSECの現在標準化が進められている点も、重要である。

3.1.5 プロキシサーバで接続先解決する方式

接続先解決を、ユーザ端末側ではなく、網側のプロキシサーバなどで行なう方式が考えられる。ユーザが求めているライフライン通信に対応するインターネットアドレスが、少なくともどこかの時点で解決されなければいけないため、それをユーザ端末側で行なわなければ、プロキシサーバなどで解決することになる。その場合は、ユーザからプロキシサーバへは、ライフラインサービスの種類の指定と地理的位置情報が渡され、その情報を利用してプロキシサーバが接続先情報管理サーバとの通信により解決することになる。

しかし、接続先解決によって得られるものは、接続すべき通信相手のメールアドレス、ウェブアドレス、SIPアドレスなど多様な通信手段のリストであることから、例えば、網側のプロキシSIPサーバといった特定のサーバが接続先解決を行なっても、そのうちのSIPアドレスしか有効に利用できない。また、ユーザ端末側では、例えば対応するメールアドレスがあるかどうかもわからないので、ユーザ端末はプロキシのメールサーバとまずは通信をしてみて、そこで初めてメールが非対応であると判明するという無駄な状況を招いてしまう。

一方、本提案方式のように、ユーザ端末側で接続先解決を行なえば、得られた通信手段のリストから利用者が選択して利用することが可能となる。この点では、今回のライフライン通信だけでなく、一般通信においてのENUMによる接続先

解決の場合も全く同様である。したがって、接続先解決は端末側でするのが好ましい。

3.2 地理的位置情報の取扱い方式における比較評価

ここでは、インターネット上における地理的位置情報の取扱い方式について、他の方式と本提案方式との比較評価についての説明を行なう。

3.2.1 網側から情報提供しない方式

網側からの地理的位置情報提供を行なわない方法では、GPS などインターネットとは別の外部から得た情報のみを元に、接続先解決を行なったり、情報通知を行なうことになる。GPS などが利用できない環境で困るだけでなく、GPS 情報を得ることができた場合においても、その情報を通信相手先に伝えたときに、情報を受け取った側では、その情報が本当に GPS から得られた情報なのかどうかを判別することができない。ライフライン通信においては、発信者の地理的位置情報についてもなりすましや間違いを防ぐ必要があるため、それを解決するためには、網側からの地理的位置情報の提供が必要であり、それによって GPS などが利用できない場合にも対応することができる。

3.2.2 DNS による情報提供方式

網側からの地理的位置情報の提供方法として、DNS において地理的位置情報を扱うレコードタイプを提案した RFC1712 (DNS Encoding of Geographical Location) [22] と、RFC1876 (A Means for Expressing Location Information in the DNS) [23] の二つが存在する。両者の主な違いは、RFC1712 では経度・緯度・高度だけなのに対し、RFC1876 では精度や大きさまで情報として含むようになっている。これらの RFC では、DNS において地理的位置情報を扱えるよう登録できる枠組みのみで、誰がどのように登録するかといった運用方法は範囲外となるが、この枠組みを利用して、二つの運用方法が考えられる。

一つは、網側が把握できる各ユーザ端末の位置をおよその位置を、網側が登録して情報提供する運用方法である。これによって、ユーザ端末だけでなく、接続先の通信相手なども直接 DNS を引くことでおよその位置の情報を取得することができ、ユーザ端末からの通知に依存することなく、直接網側が提供している情報を把握できる。

もう一つは、ユーザ端末で得られた GPS 情報などを、申請することで DNS へと登録していく運用方法である。これにより、接続先の通信相手などから見ると、DNS を検索するだけで発信者の地理的位置情報を入手することができる。

しかし、これらの DNS を利用した情報提供方法には多くの問題がある。まず、DNS による提供ではアクセス制御が困難であるため、誰でも情報を検索して調べることができ、プライバシー保護の観点から問題がある。また、移動するユーザ端末については、その地理的位置情報を次々と更新する必要があるが、DNS ではキャッシュを多用するため、登録データを更新したときの情報伝播が遅いといった問題がある。さらに、後者のユーザ端末による申請登録方式の場合、あくまでもユーザ端末からの自己申告となるため、その情報の正当性は全く保証されないことになる。

一方、本提案方式では、地理的位置情報証明書を、必要なときに必要な相手へのみ通知することで、これらの、プライバシー保護の問題・最新情報伝播の問題・情報の正当性保証の問題を解決している。

3.2.3 DHCP による情報提供方式

網側からの地理的位置情報の提供方法として、DHCP よる地理的位置情報の提供を提案した方式がある。一つは、経度・緯度・高度および各精度表現による地理的位置情報を DHCP によって提供する [20] ものであり、もう一つは、住所表現による地理的位置情報を DHCP によって提供する [21] ものである。

この DHCP による地理的位置情報提供によって、ユーザ端末は地理的位置情報を網から入手することができるため、その情報を利用してライフライン通信の接続先解決などを行なうことができる。また、ユーザ端末へと直接情報提供をするため、DNS による情報提供と異なり、プライバシー保護の問題が発生しない。

しかし、この DHCP で得られた自分の地理的位置情報をライフライン通信の通信相手へ通知した時に、通知を受けた側では、その情報は DHCP によって提供されたデータそのままで本物なのか、あるいはユーザ端末が改変して詐称しているのかを区別することができないという欠点を持つ。

一方、本提案方式では、網側よりユーザ端末へ情報提供する際に、地理的位置情報単体ではなく、地理的位置情報証明書の発行として提供しているため、それをユーザ端末から通知を受けた者は、改変がないかどうかの検証をすることができる。

3.2.4 ユーザによる情報通知方式

発信ユーザからの地理的位置情報の通知方法として、例えば、HTTP ヘッダを拡張してウェブサーバへ地理的位置情報を伝える方式 [15] が提案されている。これにより、自分の住所あるいは地域がどこかといった通知や、経度・緯度・高度がどこであるかといった通知ができるようになっており、この場合はウェブサーバがその情報を見てユーザへ最適な情報を返すことができる。例えば、周辺の地図を出したり、最寄りの店情報を提供したり、そのユーザの地域のテレビ番組表を表示したりする用途には非常に有効である。

しかし、この地理的位置情報の通知は、あくまでもユーザからの自己申告であり、いくらでもユーザによって詐称することができる。ライフライン通信の場合には、本提案方式のように、ユーザからの自己申告だけでなく、網側から保証された地理的位置情報証明書を用いるべきである。

3.2.5 サーバへの問い合わせ方式

発信ユーザの地理的位置情報の入手方法として、ユーザの地理的位置情報を把握管理するサーバなどへ、情報を問い合わせる方式が考えられる。つまり、発信ユーザ側からの情報通知を受ける方法とは異なり、ユーザの地理的位置情報を知りたい側、つまり、ライフライン通信サービス機関などが、必要に応じて問い合わせにいく方法である。

しかし、この方式を実現するには解決すべき問題が多く存在する。まずは、どこへ問い合わせに行くのかといった問題であり、例えば地理的位置情報を集中管理するサーバが損在位すればそこへ問い合わせに行けばよいが、一極集中管理をする点でスケーラビリティの問題があり、さらに、個人情報である地理的位置情報を一手に管理するサーバはプライバシー保護の観点からも問題がある。したがって、集中管理方式は現実的でなく、分散管理方式が望ましい。

次に、地理的位置情報を分散管理する方式の場合、誰がどう管理して、どこへ問い合わせに行けばよいのか、といった問題がある。例えば、発信ユーザのユーザアドレスを把握している状況において、そのユーザが所属しているホームドメイン、すなわちユーザ@ドメインのうちのドメイン部である各組織へと問い合わせに行く方法が考えられる。しかし、ユーザのホームドメイン側は常にユーザの地理的位置情報を把握しているわけではなく、ユーザは居場所を変えて無関係のアクセス用ネットワークを用いている場合もあり、ユーザのホームドメインからはユーザのおよその位置ですら一般的には把握できない。また、ユーザからホームドメインへと自分の地理的位置情報を登録する運用方法も考えられるが、ホームドメインに常に自分の居場所を把握されるプライバシー問題と、あくまでも自己申告であることから情報の正当性の問題が生じる。

また、本提案方式における保証モデルのように、ユーザが利用しているネットワーク側ではユーザのおよその位置を把握できるという原理に基づいて、ユーザの属するドメインではなく、アクセスのために使用しているネットワーク側で、情報問い合わせ受付けサーバを運用する方法が考えられる。これによって、ユーザからの自己申告情報に依存せずに、およその位置情報を提供することができるようになる。しかし、集中管理方式や、ホームドメインでの管理方式と同様に、誰からの問い合わせに対して返答をしても大丈夫なのか、といった、個人情報のプライバシーに関わる重大な問題が依然として残ってしまう。ユーザがライフライン通信を行なう等していて、そのライフライン通信を受けた側が地理的位置情報を把握してもらわなければいけない時のみ、問い合わせに応じるべきであるが、そのようなアクセス制限を行なうのは困難である。

一方、本提案方式では、地理的位置情報証明書を用いることで、このようなア

クセス制限の解決をするとともに、問い合わせに行かなくても情報の正当性を検証することができるようになっている。したがって、サーバへの問い合わせ方式よりも、地理的位置情報証明書による通知方式のほうが好ましい。

3.3 ユーザ情報の取扱い方式における比較評価

ここでは、インターネット上におけるユーザ情報の取扱い方式について、他の方式と本提案方式との比較評価についての説明を行なう。

3.3.1 サーバへの問い合わせ方式

本提案方式のようなユーザ情報証明書を用いる方法ではなく、サーバへ問い合わせる方式が考えられる。つまり、ユーザから通知された情報の正当性を確認するための問い合わせ、あるいは、ユーザ情報自体を問い合わせるといったことが考えられる。通信をしてきている以上、ユーザ識別子であるユーザアドレスが自己申告であったとしても判明しているので、そのユーザアドレスの管理ドメインに対して問い合わせを行なうことで、どこか特定サーバへの集中問い合わせといった自体は防ぐことが可能である。

しかし、各ドメインの問い合わせ受付けサーバは、問い合わせに対してするアクセス権をどうするかというプライバシー保護に関する問題を抱えてしまい、どのような時に、どのユーザについての問い合わせを、誰に対してのみ返答してよいかといった判断をすることが困難である。

一方、本提案方式では、ユーザ情報証明書を用いることで情報の正当性の検証をサーバへの問い合わせをすることなく実現するとともに、個人情報のプライバシー保護の面にも対応している。

3.3.2 ユーザ公開鍵証明書方式

同じように証明書を用いる方法として、各ユーザへユーザ公開鍵証明書を発行する方式が存在する。つまり、各ドメインにおいて全てのユーザに対して事前に

ユーザ公開鍵証明書を発行してしまい、各ユーザはそれを用いて通信相手に自分が誰であるかの証明を行なう方式である。

しかし、各ユーザが事前にユーザ公開鍵証明書の発行を受けておく必要がある。さらに、各ユーザ端末がそのユーザ公開鍵証明書を保持して通信のたびに証明書関係の処理を取扱う必要がある。これは、処理性能の低い端末にとっては大きな負荷となる。

一方、本提案方式では、各ユーザが個別にユーザ公開鍵証明書の発行を受けておく必要がなく、ユーザ情報管理サーバから必要なときにユーザ情報証明書が発行される。また、各ユーザ端末にとってユーザ情報証明書は、サーバから入手したあと特別な処理をすることなくそのままの形で通信相手へ送付することができる。

第7章　研究の総括

本章では、本研究によって得られた知見と今後の課題を述べ、研究を総括する。

1. 本研究によって得られた知見

本研究では、既存のメディアで様々な形で行なわれているライフライン通信を、インターネット上で完結できる形で実現することを目標にし、そのための基盤技術を確立することにより進めた。

まず、ライフライン通信の種類を検討し、これにより、緊急通報型、安否連絡型、安否登録・検索型、情報取得・提供型の四つに分類した。そして、それぞれにおいて必要とされる機能をモデル化し、すべての種類のライフライン通信における共通基盤モデルを抽出することができた。

次に、そこで得られた三つの課題、インターネット上での接続先解決、発信者の地理的位置情報の取扱い、発信者のユーザ情報の取扱いを対象として、四つの種類のライフライン通信における共通基盤技術の確立を目指し、インターネット以外の既存のメディアとインターネットにおける違いや、インターネット上の既存技術における問題点などを議論し、三つの課題それぞれを解決するにあたっての要求事項を整理することができた。

そして、それらの要求事項を満たすものとして、インターネット上での接続先解決方法としては地理的位置情報ベースの ENUM 方式、発信者の地理的位置情報を取扱う方法としては地理的位置情報証明書方式、発信者のユーザ情報を取扱う方法としてはユーザ情報証明書方式を、新たなモデルとして設計提案することができた。

それらの提案した方式によるアーキテクチャ仕様に基づき、発信者端末、地理

的位置情報管理サーバ、ユーザ情報管理サーバ、接続先情報管理サーバ、着信先端末からなる、ライフライン通信システムの設計と実装を行なった。そして、このシステムを用いた実証実験用ネットワークを構築し、実証実験による評価を行なった。

本提案方式は、インターネットの標準的なプロトコルや枠組みをベースに、インターネットの基本構成要素である IP アドレスやドメイン名の階層的な枠組みに添った形で構成されており、それに加えて新たなアイデアにてインターネット上で地理的位置情報を取り扱っている。そして、他の既存方式や考えられる方式と比較して、スケーラビリティが高く考慮されたものであるとともに、、セキュリティとプライバシーにも考慮された方式であることを示すことができた。また、システムの性能測定の結果、本提案によって導入した証明書の取り扱いによるオーバーヘッドを含めても十分実用的な時間と負荷でシステムが動作することを示すことができた。

2. 今後の課題

本研究により、様々なタイプのライフライン通信においてインターネット上で必要となる共通基盤を確立することができた。しかし、本研究では代替アプローチをとることで対象外とした (第 2 章第 2.1.4 節)、優先取扱いによる通信品質確保などの問題が別途残っている。今後、それらの分野の研究が更に進められる必要があるとともに、本研究の成果との融合が課題として挙げられる。

本研究のライフライン通信システム自体の拡張としては、第 5 章のシステムの拡張のところで述べた、モバイル IP への対応などの詳細設計を検討するとともに、実証していく必要がある。

また、本研究で対象とした、インターネットだけで完結できるライフライン通信のシステムを実社会において実現していくには、その運用体制などを社会的な面から更に掘り下げていく必要があり、同時に、その配備コストなども議論しながら、実用的な普及展開モデルを検討していく必要がある。

3. 結論

本研究では、インターネットにおけるライフライン通信の実現にあたって、ライフライン通信の分類とモデル化、必要となる機能、既存技術での問題、解決するための要求事項を議論し、その要求事項を満たす各提案方式と、それらに基づいて設計されたライフライン通信システムを提案した。また、このライフライン通信システムを実際に実装構築し、実証実験と性能測定によって実用的に利用可能なことを示した。これらにより、本研究で得られた成果は、インターネット上でライフライン通信を実現するために必要な基盤技術の確立となるとともに、今後の更なる研究のために大きく寄与するものと考える。

謝辞

本研究を進めるにあたり、多くの皆さまからご協力とご助言をいただきました。ここに感謝の意を表します。

本研究を行なう機会を与えて下さり、研究内容に関しても多大なるご指導をいただきました、奈良先端科学技術大学院大学 情報科学センターの砂原秀樹 教授に、心より深く感謝いたします。

また、本研究のご指導をいただきました、奈良先端科学技術大学院大学 情報科学研究科の山口英 教授、奈良先端科学技術大学院大学 情報科学センターの藤川和利 助教授に、厚く御礼申し上げます。

本研究を始める機会を与えて下さるとともに、本研究に対して多大なるご指導とご支援をして下さいました、KDDI 研究所の浅見徹 所長と山崎克之 室長に、深く感謝いたします。

本研究の多くの部分は、通信・放送機構の直轄研究開発プロジェクトである、IP ネットワーク上でのライフラインの実現のための研究開発プロジェクトのもとで行ないました。ご指導・ご協力いただきました、プロジェクトリーダーである大阪大学の下條真司 教授、ならびに、野呂正明 研究員を始め多くの方々に対し、心より感謝いたします。

様々な形でお世話になりました、奈良先端科学技術大学院大学 情報科学研究科 インターネット・アーキテクチャ講座の研究室のみなさま方、特に、様々なアドバイスを下さった和泉順子 女史、色々とフォローをして下さった能勢佳苗 女史に感謝いたします。

最後に、本学在学途中で亡くなった父と、その後も支えてくださった母に、感謝と御礼を申し上げます。

研究業績

学術論文

1. Takahiro Kikuchi, Masaaki Noro, Katsuyuki Yamazaki, Hideki Sunahara, Shinji Shimojo, “Design and Implementation of Lifeline Communication System in the Internet”, IEICE Transactions on Information and Systems, Vol.E87-D, No.12, pp.2714–2722, December 2004.

国際会議 (査読付)

1. Tohru Asami, Takahiro Kikuchi, Kenji Rikitake, Hiroshi Nagata, Tatsuaki Hamai, Yoshinori Hatori, “A Taxonomy of Spam and a Protection Method for Enterprise Networks”, Proceedings of the 16th International Conference on Information Networking (ICOIN16), pp.3B-4.1–11, January 2002.

2. Takahiro Kikuchi, Masaaki Noro, Hideki Sunahara, Shinji Shimojo, “Lifeline Support of the Internet”, Proceedings of 2003 Symposium on Applications and the Internet (SAINT2003) Workshops, IEEE Computer Society, pp.323–327, January 2003.

3. Takahiro Kikuchi, Masaaki Noro, Katsuyuki Yamazaki, Hideki Sunahara, Shinji Shimojo, “Lifeline Communication System in the Internet”, Proceedings of 2004 Symposium on Applications and the Internet (SAINT2004) Workshops, IEEE Computer Society, pp.236–242, January 2004.

国内発表

1. 菊地 高広, 浅見 徹, 力武 健次, 永田 宏, 濱井 龍明, “IP アドレス詐称対策のためのリバースパスによるフィルタリング手法”, Proceedings of IPSJ Computer Security Symposium 2001 (CSS2001), pp.191–196, October 2001.

2. 浅見 徹, 菊地 高広, 力武 健次, 永田 宏, 濱井 龍明, 羽鳥 好律, “企業網における SPAM 対策と実現手法”, Proceedings of IPSJ Computer Security Symposium 2001 (CSS2001), pp.139–144, October 2001.

3. 菊地 高広, 野呂 正明, 砂原 秀樹, 下條 真司, “インターネットにおけるライフラインの実現”, インターネットコンファレンス 2002 論文集, pp.116, October 2002.

4. 野呂 正明, 菊地 高広, 大熊 秀明, 砂原 秀樹, 下條 真司, “インターネットにおけるライフライン機能の実現”, 電子情報通信学会技術研究報告 IA2003-15, pp.9–15, July 2003.

その他

1. 菊地 高広, 野呂 正明, 大熊 秀明, 小野寺 充, 菊川 泰士, 砂原 秀樹, 下條 真司, 他, “IP ネットワーク上でのライフラインの実現のための研究開発 最終報告書”, 通信・放送機構, pp.1–354, March 2004.

2. 菊地高広, “ライフライン通信における接続先解決と発信者情報通知”, VoIP 推進協議会第 11 回全体会合研究成果発表会, April 2004.

参考文献

[1] Takahiro Kikuchi, Masaaki Noro, Hideki Sunahara, Shinji Shimojo, “Lifeline Support of the Internet”, Proceedings of 2003 Symposium on Applications and the Internet (SAINT2003) Workshops, IEEE Computer Society, pp.323–327, January 2003.

[2] 野呂 正明, 菊地 高広, 大熊 秀明, 砂原 秀樹, 下條 真司, “インターネットにおけるライフライン機能の実現 “, 電子情報通信学会技術研究報告 IA2003-15, pp.9–15, July 2003.

[3] 大熊 秀明, 小野寺 充, 菊川 泰士, 砂原 秀樹, 下條 真司, “障害発生時の VoIP 音声品質の検討と評価 “, 電子情報通信学会技術研究報告 IA2003-40, pp.25–30, January 2004.

[4] Masaaki Noro, Takahiro Kikuchi, Ken-ichi Baba, Hideki Sunahara, Shinji Shimojo, “QoS Support for VoIP Traffic to Prepare Emergency”, Proceedings of 2004 Symposium on Applications and the Internet (SAINT2004) Workshops, IEEE Computer Society, pp.229–235, January 2004.

[5] Takahiro Kikuchi, Masaaki Noro, Katsuyuki Yamazaki, Hideki Sunahara, Shinji Shimojo, “Lifeline Communication System in the Internet”, Proceedings of 2004 Symposium on Applications and the Internet (SAINT2004) Workshops, IEEE Computer Society, pp.236–242, January 2004.

[6] Nobuhiko Tada, Yukimitsu Izawa, Masahiko Kimoto, Taro Maruyama, Hiroyuki Ohno, Masaya Nakayama, “IAA System (I Am Alive): The Experiences of the Internet Disaster Drills”, Proceedings of INET2000, July 2000.

[7] Postel, J., "Internet Protocol", RFC 791, September 1981

[8] Mockapetris, P., "Domain names - concepts and facilities", RFC 1034, November 1987

[9] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E., "SIP: Session Initiation Protocol", RFC 3261, June 2002

[10] Berners-Lee, T., Fielding, R., Masinter, L., "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998

[11] Rosenberg, J., Schulzrinne, H., "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002

[12] Faltstrom, P., Mealling, M., "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761, April 2004

[13] ITU-T, "The International Public Telecommunication Number Plan", Recommendation E.164, ITU, May 1997

[14] Mealling, M., "Dynamic Delegation Discovery System (DDDS)", RFC 3401-3404, October 2002

[15] Andrew Daviel, BSc., "Geographic extensions for HTTP transactions", draft-daviel-http-geo-header-04, Internet Draft, July 2003

[16] Andrew Daviel, BSc., "Geographic registration of HTML documents", draft-daviel-html-geo-tag-06, Internet Draft, July 2003

[17] Sohgo Takeuchi, Yasuhito Watanabe, Fumio Teraoka, "The GLI System: A Global System Managing Geographical location information of Mobile Entities", Proceedings of the 3rd International Symposium on Wireless Per-

sonal Multimedia Communications (WPMC2000), IEEE, Bangkok, Thailand, November 2000, pp.1073-1078

[18] Michiko Izumi, Sohgo Takeuchi, Yasuhito Watanabe, Keisuke Uehara, Hideki Sunahara, Jun Murai, "A Proposal on a Privacy Control Method for Geographical Location Information Systems", Proceedings of INET 2000, Internet Society, Yokohama, Japan, June 2000

[19] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997

[20] Polk, J., Schnizlein, J., Linsner, M., "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004

[21] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", draft-ietf-geopriv-dhcp-civil-04, Internet Draft, September 2004

[22] Farrell, C., Schulze, M., Pleitner, S., Baldoni, D., "DNS Encoding of Geographical Location", RFC 1712, November 1994

[23] Davis, C., Vixie, P., Goodwin, T., Dickinson, I., "A Means for Expressing Location Information in the Domain Name System", RFC 1876, January 1996

[24] IEC, "Maritime navigation and radiocommunication equipment and systems - Digital interfaces", IEC 61162-1 (NMEA 0183), IEC, July 2000

[25] P. Bahl and V. N. Padmanabhan, "RADAR: An In-Building RF-Based User Location and Tracking System", Proceedings of the IEEE Infocom 2000, Vol.2, pp.775-784, March 2000.

[26] Donovan, S., "The SIP INFO Method", RFC 2976, October 2000

[27] Johnson, D., Perkins, C., Arkko, J., "Mobility Support in IPv6", RFC3775, June 2004

[28] Housley, R., Polk, W., Ford, W., Solo, D., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002

[29] Ramsdell, B., "S/MIME Version 3 Message Specification", RFC 2633, June 1999

[30] Partridge, C., Mendez, T., Milliken, W., "Host Anycasting Service", RFC 1546, November 1993